Montana Law Review

Volume 37
Issue 1 *Winter 1976*

Article 3

1-1-1976

A Growing Awareness of Privacy in America

Thomas E. Towe
Senator, District 34, 1975 Montana Legislature

A GROWING AWARENESS OF PRIVACY IN AMERICA

Thomas E. Towe*

I. PRIVACY IN AMERICAN JURISPRUDENCE

There is developing a national consensus on the importance of privacy. It has not always been so. In fact, privacy did not even emerge as a separate concept until the close of the American frontier in the last part of the 19th century.

Nowhere is the word "privacy" mentioned in the Magna Carta, the English Bill of Rights or any of the other documents normally considered a part of our legal tradition. Nowhere is reference made to "privacy" or to any similar concept in the writings of Locke, Rousseau, Montesquieu or other political philosophers who had a profound influence on the Founding Fathers of this nation. In fact, nowhere is privacy mentioned in the Constitution of the United States or any of its 26 amendments. A review of the works of Thomas Jefferson, James Madison, Alexander Hamilton, John Adams and other Founding Fathers reveals that "privacy" was not one of their major concerns in releasing the American people from the shackles of colonial rule.[1]

Privacy, as a separate legal concept, first appeared over 100 years after this nation was born when Samuel Warren and Louis Brandeis wrote an article entitled "The Right to Privacy" for the HARVARD LAW REVIEW in 1890.[2] It was another fifteen before any court gave privacy full and independent status.[3] From this slow beginning, the right of privacy is now recognized in the tort law of at least forty-three states and the District of Columbia.[4]

---

*B.A., Earlham College; LL.B., University of Montana; LL.M., Georgetown University, and Candidate for S.J.D., University of Michigan. Mr. Towe is an attorney in Billings, Montana, and was elected to the 1975 Montana Legislature as Senator from District 34.

1. *But see Griswold v. Connecticut*, 381 U.S. 479 (1965) in which Justice Douglas argues that although the founding fathers did not use the word "privacy", they certainly had this concept in mind in drafting the First, Third, Fourth, Fifth and Ninth Amendments. It is reasonable to suggest, for example, that James Otis was really concerned about "privacy" when he argued against the Writs of Assistance which allowed officers of the Crown to search any colonist's home without justification.

2. Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

3. Pavesich v. New England Life Insurance Co., 122 Ga. 190, 50 S.E. 68 (1905). Privacy was given partial recognition by statute in New York in 1903. N.Y. SESS. LAWS, 1903, ch. 132 §§ 1-2; N.Y. Civ. Rights Law §§ 50-51 (McKinney 1948).

4. 27 jurisdictions had recognized the right of privacy by 1960: Alabama, Alaska, Arizona, California, Connecticut, the District of Columbia, Florida, Georgia, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Michigan, Mississippi, Missouri, Montana, Nevada, New Jersey, North Carolina, Ohio, Oregon, Pennsylvania, South Carolina, Tennessee and West Virginia. *See* Prosser, *Privacy*, 48 CALIF. L. REV. 383, 386 (1960). Since then it has officially been recognized in Delaware: *Barbiere v. Navo-Journal Co.*, 189 A.2d 773 (1963); Maryland: *Carr v. Watkins*, 227 Md. 578, 197 A.2d 841 (1964); Arkansas: *Olan Mills v. Dodd*,

Privacy first appeared in the language of the decisions of the Supreme Court in *Boyd v. United States*, decided in 1886.[5] Reference to "the privacies of life," however, was made for the purpose of defining and establishing parameters of the Fourth Amendment right to be free from unauthorized searches and seizures.[6] The relationship between privacy and the Fourth Amendment is now firmly established.[7] The Supreme Court has examined the invasion of privacy involved in a particular case to determine if a person has standing under the Fourth Amendment,[8] to determine whether a search without a warrant can be justified,[9] to determine the scope

---

234 Ark. 495, 353 S.W.2d 22 (1961); South Dakota: *Traxes v. Kenco Enterprises*, 80 S. Dak. 104, 119 N.W.2d 914 (1963); New Hampshire: *Hamberger v. Eastman*, 106 N.H. 107, 206 A.2d 239 (1964); Hawaii: *Fergerstrom v. Hawaiian Ocean View Estates*, 50 Haw. 374, 441 P.2d 141 (1968); and Texas: *Billings v. Atkinson*, 489 S.W.2d 858 (1973). The right of privacy has been recognized in four states by legislation: New York, Oklahoma, Utah and Virginia. *See* Prosser, at 388. Additionally, 6 states, Colorado, Idaho, Massachusetts, Minnesota, New Mexico and Washington, have decided cases on privacy, but the cases, without rejecting the right of privacy, were resolved on other grounds. *See* Prosser, at 386; *Hubbard v. Journal Pub. Co.*, 69 N. Mex. 473, 368 P.2d 147 (1962). Privacy as a tort concept has been expressly rejected in only 3 states: Nebraska: *Brunson v. Ranks Army Store*, 161 Neb. 519, 73 N.W.2d 803 (1955); Rhode Island: *Henry v. Cherry & Webb*, 30 R.I. 13, 73 A. 97 (1909) and Wisconsin: *Judevine v. Benzies Montanye Fuel & Warehouse Co.*, 222 Wis. 512 (1956), 269 N.W. 295 (1936) and *Yoeckel v. Samonig*, 262 Wis. 430, 75 N.W.2d 925 (1956). Although Wisconsin claims not to recognize a tort action for invasion of privacy, the cases seem to reach the same conclusion under the theory of severe emotional stress caused by outrageous conduct. *Alsteen v. Gehl*, 21 Wis.2d 349, 356, 124 N.W.2d 312, 316 (1963) and *Slarvek v. Stroh*, 62 Wis.2d 295, 215 N.W.2d 9, 20 (1974). No cases have been decided on the issue in Maine, North Dakota, Vermont and Wyoming. *See generally* DON R. PEMBER, PRIVACY AND THE PRESS at Appendix C (University of Washington Press 1972).

5. 116 U.S. 616, 630 (1886).

6. Justice Bradley refers to "the sanctity of a man's home and the privacies of life" in declaring a federal statute that compelled the production of private books and papers unconstitutional. 116 U.S. at 630. Conceivably he acquired the concept from COOLEY, CONSTITUTIONAL LIMITATIONS at 304 (1868). Professor Cooley states: "The law requires the utmost particularity in these cases before the privacy of a man's premises is allowed to be invaded by the minister of the law."

7. Wolf v. Colorado, 338 U.S. 25, 27 (1949); Jones v. United States, 357 U.S. 493, 498 (1958); Abel v. United States, 362 U.S. 217, 255 (1960) (Brennan, J., dissenting); Mapp v. Ohio, 367 U.S. 643, 655 (1961); Tehan v. Shott, 382 U.S. 406, 415 (1966); Warden v. Hayden, 387 U.S. 294, 304 (1967); Katz v. United States, 389 U.S. 347, 350 (1967); Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics, 403 U.S. 488, 490 (1971) (Harlan, J., dissenting); United States v. Dionisio, 410 U.S. 1, 14 (1973); Cardwell v. Lewis, 417 U.S. 583, 591 (1974). *See also* cases at notes 8-11.

8. Jones v. United States, 362 U.S. 257, 261 (1960); Wong Sun v. United States, 371 U.S. 471 (1963); Berger v. New York, 388 U.S. 41, 101 (1967) (Harlan, J., dissenting); Mancusi v. DeForte, 392 U.S. 364, 372 (1968) (Black, J., dissenting); Alderman v. United States, 394 U.S. 165, 170, 206 (1969).

9. McDonald v. United States, 335 U.S. 451, 455-56 (1948); Camara v. Municipal Court, 387 U.S. 523, 529, 534 (1967); Berger v. New York, *supra* note 8 at 63; Terry v. Ohio, 392 U.S. 1, 21 (1968); Chimel v. California, 395 U.S. 752, 761, 766 (n. 12), 776 (1969); United States v. White, 401 U.S. 745, 789 (1971) (Harlan, J., dissenting); Cardwell v. Lewis, *supra* note 7.

of the privilege against self-incrimination,[10] and to determine the scope of the First Amendment concept of a preserve for ideas and beliefs.[11]

Privacy as a separate constitutional right has only recently been recognized. Although Justice Brandeis, as early as 1928, spoke of "the right to be let alone—the most comprehensive of rights and the most valued by civilized men," these words were in a dissenting opinion.[12] In fact, much of the law on Constitutional privacy is contained in dissenting opinions which are far better known than many majority opinions.[13]

In 1965 privacy was given explicit recognition as a constitutional right in *Griswold v. Connecticut*.[14] In that case the Supreme Court struck down a Connecticut statute prohibiting the use of birth control devices. Justice Douglas, writing for the Court, articulated the concept that even though "privacy" is not mentioned in the Constitution or the Bill of Rights, other guarantees specifically mentioned in the Bill of Rights have "penumbras" which include privacy within the scope of their protection. Zones of privacy are created by and included within the penumbras of the First Amend-

10. Miranda v. Arizona, 384 U.S. 436, 460 (1966). *See* Tehan v. Shott, *supra* note 7 at 315, 416; Schmerber v. California, 384 U.S. 757, 762 (1966); Bellis v. United States, 417 U.S. 85 (1974).

11. Schneider v. Smith, 390 U.S. 17, 25, 27 (1968). Although the Court does not actually use the term "privacy," it refers to "a preserve where the views of the individual are made inviolate." 390 U.S. at 25.

12. Olmstead v. United States, 277 U.S. 438, 478 (1928).

13. *See* Justice Murphy's dissent in *Goldman v. United States*, 316 U.S. 114, 136 (1942); Justice Frankfurter's dissents in *Davis v. United States*, 328 U.S. 582, 594 (1946) and *Rabinowitz v. United States*, 339 U.S. 56, 68 (1950); Justices Frankfurter, Murphy, and Jackson dissenting in *Harris v. United States*, 331 U.S. 145, 155, 183, 195 (1947); Justice Burton dissenting in *On Lee v. United States*, 343 U.S. 747, 765 (1952); Justice Harlan dissenting in *Poe v. Ullman*, 367 U.S. 497, 522 (1961); Justice Douglas's dissents in *Frank v. Maryland*, 359 U.S. 360, 374 (1959), *Poe v. Ullman*, at 509, 522, and *United States v. Vuitch*, 402 U.S. 62, 74 (1973); and Justice Brennan's dissent in *Lopez v. United States*, 373 U.S. 427, 446 (1963). The 100 significant cases on privacy decided since June 7, 1965, have produced 344 separate opinions.

With the exception of Lopez, involving the use of a hidden microphone with one party consent, and *Davis*, where the Justices disagreed on the facts, the majority opinions in each of these cases have now been overruled. *See Chimel v. California, supra* note 9, overruling *Harris* and *Rabinowitz; Katz v. United States, supra* note 7, overruling *Goldman; Berger v. New York, supra* note 8, overruling *Olmstead; See v. City of Seattle*, 387 U.S. 541 (1967) and *Camara v. Municipal Court, supra* note 9, overruling *Frank; Griswold v. Connecticut*, 381 U.S. 479 (1965); replacing *Poe, Roe v. Wade*, 410 U.S. 113 (1973), replacing *Vuitch*. Although *On Lee* has not been expressly overruled, four justices in *Lopez* said they would now do so, which, when added to the dissent filed by Justice Black in *On Lee*, produces a majority for overruling the case. For a discussion on whether or not *On Lee* has been overruled, *see United States v. White, supra* note 9, where four justices say no and three say yes with Justice Black expressing no opinion on the matter. The court in *Katz* appears to have adopted the rationale of Justice Brennan's dissent in *Lopez*, although *Lopez* itself has not been overruled.

14. 381 U.S. 479 (1965).

ment (privacy of association), the Third Amendment (quartering troops in private homes), the Fourth Amendment (protection of persons, houses, papers and effects from unreasonable searches and seizures), the Fifth Amendment (the privilege against self incrimination), and the Ninth Amendment (enumeration of certain rights shall not exclude others).[15]

Justice Goldberg, concurring in *Griswold*, suggested that he would be content to rely simply on the Ninth Amendment. According to him, to deny constitutional status to a "right so basic and fundamental and so deep-rooted in our society as the right of privacy", merely because it is not expressly guaranteed, is to ignore the Ninth Amendment.[16] Justices Harlan and White, also concurring, preferred to rely on the concept of liberty protected by the Due Process Clause of the Fourteenth Amendment; they carefully avoided the use of the word "privacy."[17]

Regardless of the theory, the right of privacy is now firmly established as an independent right. It has been applied in *Eisenstadt v. Baird* (striking down the Massachusetts contraceptive law),[18] *Roe v. Wade* (striking down state abortion laws),[19] and *Cleveland Board of Education v. La Fleur* (striking down mandatory maternity leave).[20]

Privacy does not appear to have been an important concept to Americans in 1789 or 1791. The first significant cases decided by the Supreme Court involving the Fourth Amendment arose just as America's western frontier was closing.[21] However, by the last quarter of the twentieth century, as the nation's population ap-

15. 381 U.S. at 484. *See also* Doe v. Bolton, 410 U.S. 179, 212 (1973) (Douglas, J., concurring); Wisconsin v. Yoder, 406 U.S. 205 (1972). Although Chief Justice Burger insists that privacy is not the basis for the decision, *Yoder* declares invalid a state law requiring *public* education, and thus would appear to be a privacy case because it prohibits the state from interfering with the private realm of family life, namely the parents' free choice in the upbringing of their children.

16. 381 U.S. at 486, 491.

17. 381 U.S. at 499, 502.

18. 405 U.S. 438 (1972).

19. 410 U.S. 113 (1973). Justice Blackmun, writing for the Court, makes no attempt to justify privacy as a separate and independent right but simply states, the right of privacy, "is broad enough to encompass a woman's decision whether or not to terminate her pregnancy." 410 U.S. at 153.

20. 414 U.S. 632 (1974). Justice Stewart does not use the word "privacy", but he cites the principal privacy cases. 414 U.S. at 640.

21. In re Jackson, 96 U.S. 727 (1878); Boyd v. United States, 116 U.S. 616 (1886). Earlier cases were not significant. *See, e.g.*, Ex parte Buford, 3 Cranch 448 (1806); United States v. Bollman, 4 Cranch 75 (1807); Luther v. Borden, 7 How. 1 (1849). *See also* A. Westin, *Privacy and American Law: The Search for Lost Doctrine in the Computer Age* at 5, *Privacy in Western History: from the Age of Pericles to the American Republic* at 333-340, parts of a report prepared for the Project on the Impact of Technology on Privacy, Special Committee on Science and the Law, Association of the Bar of the City of New York (1965).

proached 230,000,000, the right of privacy achieved critical importance. Currently, a major portion of the Supreme Court's efforts each year are devoted to interpretation of the Fourth Amendment.[22]

II. Privacy in State Constitutions

A number of state constitutions contain more explicit provisions than the federal constitution concerning the protection of privacy. For example, Article 1, Section 7 of the original constitution for the State of Washington, adopted in 1889, after the Supreme Court's decision in *United States v. Boyd*,[23] states:

> *Invasion of Private Affairs or Home Prohibited.*
> No person shall be disturbed in his private affairs, or his home invaded, without authority of law.

Similarly, Article 2, Section 8 of the Arizona Constitution, adopted in 1910, states:

> No person shall be disturbed in his private affairs, or his home invaded, without authority of law.

New York's constitution, adopted in 1939, eleven years after the Supreme Court's decision in *Olmstead v. United States*,[24] contains a special provision relating to interception of communications.

> The right of the people to be secure from unreasonable interceptions of telephone and telegraph communications shall not be violated, and ex parte orders or warrants shall issue only upon oath or affirmation that there is reasonable ground to believe that evidence of a crime may be thus obtained, and identifying the particular means of communication, and particularly describing the person or persons whose communications are to be intercepted and the purpose thereof.[25]

The new Florida constitution also specifically refers to interception of communications,[26] while wiretapping is specifically prohibited in

22. For example, in the October Term, 1972, the Court handed down 177 written opinions, 17 of which dealt with the Fourth Amendment in some manner.

23. 116 U.S. 616 (1886).

24. 277 U.S. 438 (1928).

25. N.Y. Const. art. 1, § 12.

26. Florida Const. art. 1, § 12 (1968), which provides:
Searches and Seizures. The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures and against the unreasonable interception of private communications by any means, shall not be violated. No warrant shall be issued except upon probable cause, supported by affidavit, particularly describing the place or places to be searched, the person or persons, thing or things to be seized, the communications to be intercepted, and the nature of the evidence to be obtained. Articles or information to be obtained in violation of this right shall not be admissible for evidence.

Puerto Rico.[27]

Constitutions in six states, all adopted since 1970, refer specifically to "privacy." They are:

Alaska: The right of the people to privacy is recognized and shall not be infringed. The legislature shall implement this section.[28]
California: All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.[29]
Hawaii: The rights of the people to be secure in their persons, houses, papers and effects against unreasonable searches, seizures, and invasions of privacy shall not be violated; and no warrants shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized or the communications sought to be intercepted.[30]
Illinois: *Search, Seizure, Privacy and Interceptions.* The people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, invasions of privacy or interceptions of communications by eavesdropping devices or other means. No warrant shall issue without probable cause, supported by affidavit particularly describing the place to be searched and the persons or things to be seized.[31]
Right to Remedy and Justice. Every person shall find a certain remedy in the laws for all injuries and wrongs which he receives to his person, privacy, property or reputation. He shall obtain justice by law, freely, completely, and promptly.[32]
Montana: *Right of Privacy.* The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest.[33]
Right to Know. No person shall be deprived of the right to examine documents or to observe the deliberations of all public bodies or agencies of state government and its subdivisions, except in cases in which the demand of individual privacy clearly exceeds the merits of public disclosure.[34]
South Carolina: *Searches and Seizures: Invasions of Privacy.* The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures and unreasonable invasions of privacy shall not be violated, and no

27. PUERTO RICO CONST. art. II, § 10.
28. ALASKA CONST. art. I, § 2 (1972).
29. CAL. CONST. art. 1, § 1 (1974).
30. HAWAII CONST. art. 1, § 5 (1968).
31. ILL. CONST. art. 1, § 6 (1970).
32. ILL. CONST. art. 1, § 12 (1970).
33. MONT. CONST. art. II, § 10 (1972).
34. MONT. CONST. art. II, § 9 (1972).

warrants shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, the person or thing to be seized, and the information to be obtained.[35]

Although Hawaii, Illinois, and South Carolina have merely added the concept of privacy to the existing search and seizure provisions, and California has merely applied the concept of privacy to the existing inalienable rights provision, Alaska and Montana have both created entirely new sections which provide separate status and treatment for the right. Also, Illinois seems to raise the tort right of privacy to a constitutional level in Section 12, "Right to Remedy and Justice." Only Montana has attempted to confront the problem of conflict between the citizens' right to know and the citizens' right to privacy in Section 9, "Right to Know." It is safe to suggest that future constitutional drafts and proposals will invariably mention the word "privacy". Most will contain a special section devoted to privacy.

III. Privacy in Congress

The first major action by Congress pertaining to privacy came in 1934, just six years after the Supreme Court upheld the practice of wiretapping in *Olmstead v. United States*.[36] In 1934 Congress prohibited wiretapping by passage of § 605 of the Federal Communications Act.[37] Since then, and particularly in recent years, Congress has engaged in a flurry of activity on a number of subjects relating to privacy.

A. Wiretapping and Eavesdropping: Title III of the Omnibus Crime Control and Safe Streets Act of 1968

Since 1934 over 100 bills regarding wiretapping have been introduced in Congress.[38] Hearings on that subject have been extensive; over three thousand pages of testimony were taken between 1958 and 1962 in the various subcommittees of the Senate Committee on the Judiciary.

The result was a major new wiretap law, Title III of the Omnibus Crime Control and Safe Streets Act of 1968. It prohibits all wiretapping and electronic interception of communications except by law enforcement officers for certain crimes under court order, granted upon probable cause. Such surveillance is carefully con-

35. S.C. Const. art. 1, § 10 (1971).

36. *Supra*, note 12.

37. 47 U.S.C. § 605.

38. *See, e.g.* H.R. 14564, H.R. 16896, H.R. 16985, H.R. 17617, 93rd Congress; S. 1888, 94th Congress.

trolled by limiting the persons who can authorize it and by imposing strict reporting requirements. Certain exceptions are made for national security cases. State law enforcement officers are similarly limited to interceptions authorized by a prior court order. The manufacture, sale, and possession of any devices designed for surreptitious interception of communications is a criminal offense under the act, and civil remedies are granted to victims of unlawful interceptions.[39]

Although the act is progressive in its prohibition of wiretapping, the exception for law enforcement officers has been the subject of much criticism.[40] The official reporting required under the act reveals a great deal of surreptitious electronic surveillance by the police. In 1974, 694 taps were authorized for an average twenty-six days each at an average cost of about $8,000. Of these taps, 120 were placed by federal officers and 574 were placed by state and local officers.[41]

Additional criticism has been leveled at the exception for national security on the charge that the exception has been badly abused.[42] Annually, Senator Edward Kennedy releases figures obtained from the Department of Justice on government wiretaps installed for national security purposes. Prior to 1974 the number averaged 111 per year, but it jumped to 190 taps in 1974.[43]

The National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance, a commission contemplated by the Omnibus Crime Control and Safe Streets Act of 1968 to review the operation of that portion of the Act relating to wiretapping and electronic surveillance, discovered an-

39. 18 U.S.C. §§ 2511-2520.

40. *See, e.g.* THE NEW REPUBLIC, May 18, 1968, at 4; Herman Schwartz, *The Legitimation of Electronic Eavesdropping: The Politics of "Law and Order,"* 67 MICH. L. REV. 455 (1969); EDITH LAPIDUS, EAVESDROPPING ON TRIAL, (Hayden Book Co. 1974); RAMSEY CLARK, CRIME IN AMERICA (Simon and Schuster 1974); HERMAN SCHWARTZ, A REPORT ON THE COSTS AND BENEFITS OF ELECTRONIC SURVEILLANCE—1972 (American Civil Liberties Union, 22 East 40th St., New York, N.Y. 10016, 1974).

41. Report, *Applications for Orders Authorizing or Approving the Interception of Wire or Oral Communications, 1974*, issued by the Director of the Administrative Office of the United States Courts. *See also*, PRIVACY JOURNAL, No. 9, July 1975, p. 1 (P.O. Box 8844, Wash. D.C. 20003.)

42. *Hearings on Warrantless Wiretapping Before the Subcomm. on Administrative Practice and Procedure of the Senate Comm. on the Judiciary*, 92d Cong., 2d Sess. (1972); SUBCOMM. ON SURVEILLANCE OF THE SENATE FOREIGN RELATIONS COMM. AND THE SUB-COMM. ON ADMINISTRATIVE PRACTICE AND PROCEDURE OF THE SENATE COMM. ON THE JUDICIARY, WARRANTLESS WIRETAPPING AND ELECTRONIC SURVEILLANCE, 94th Cong., 1st Sess., (Comm. Print 1975); *The Impeachment Inquiry of the House Comm. on the Judiciary*, 93d Cong., 2d Sess. (1974) at Book VII; P. COWAN, N. EGLESON, AND N. HENTOFF, STATE SECRETS (Holt, Rinehart & Winston 1970); (Hearings on Dr. Kissinger's Role in Wiretapping Before the Senate Foreign Relations Comm., 93d Cong., 1st and 2d Sess. (1972-73).

43. PRIVACY JOURNAL, *supra* note 41.

other problem. At hearings on June 27, 1975, the American Telephone and Telegraph Co. revealed that between 1967 and 1974, it discovered 1457 wiretaps on customers' telephones including 1009 illegal devices, about eighty-three precent of which were installed in residences.[44]

Based on these and other figures, PRIVACY JOURNAL has estimated that a minimum of 1052 wiretaps were installed in 1974 which intercepted 1.9 million conversations.[45] This figure does not include conversations overheard by electronic microphones (bugs) installed without connection to a telephone line. In 1974, at least 42 bugs were installed for national security purposes.[46] We have a long way to go before the privacy and security of our oral communications are assured.

B. Polygraph Tests: There Is No Lie Detector (The Moss Subcommittee)

In 1964 and 1965, hearings were held on the use of polygraphs as "lie detectors" by the federal government before the Foreign Operations and Government Information Subcommittee of the House Committee on Government Operations (Moss Subcommittee).[47] After hearing extensive testimony, the committee concluded: "There is no 'lie detector,' neither machine nor human. People have been deceived by a myth that a metal box in the hands of an investigator can detect truth or falsehood."[48]

The committee further discovered that the federal government was spending several million dollars on polygraph machines and the employment of full time operators. Most of the operators were not properly qualified to operate the machines. In addition, many of the examinations were completely outside the scope of national security. The government was planning to expand use of such examinations without any attempt to verify the machine's accuracy or usefulness.[49] Individuals under interrogation were persuaded to disclose

---

44. *Id.*

45. *Id.*

46. *Id.*

47. *Hearings on the Use of Polygraphs as "Lie Detectors" Before the Foreign Operations and Government Information Subcomm. of the House Comm. on Government Operations*, 88th Cong., 2d Sess. (1964), 89th Cong., 1st Sess. (1965).

48. H.R. REP. No. 89-198, 89th Cong., 1st Sess. (1965) at 1. *See also*, H.R. REP. No. 80-2081, 89th Cong., 2d Sess. (1966); HOUSE COMM. ON GOVERNMENT OPERATIONS, 88TH CONG., 2D SESS., USE OF POLYGRAPHS BY THE FEDERAL GOVERNMENT (PRELIMINARY STUDY) (Comm. Print 1964).

49. The committee received the report of a young branch manager of a bank who flunked the "routine" polygraph test. He took it two more times and failed. The fourth time the examiner pinpointed the amount of money alleged to have been stolen or embezzled at $800 to $1100. The manager was thoroughly confused and could not recall anything about the alleged wrongdoing. However, in the belief that the machine could not be fooled, he

past indiscretions and the use of two-way mirrors and hidden microphones to study the subject's reaction more carefully was becoming increasingly common.

Perhaps the most dramatic invasion of privacy was reported by Representative Cornelius Gallagher from New Jersey. A seventeen year old female, who applied for a non-sensitive job at a non-security government agency, was given a lie detector test by a twenty-one year old male who inquired extensively into her sex life.[50] The committee recommended prohibiting use of polygraph examination except in the most serious national security and criminal cases, requiring that they be completely voluntary, and insuring that refusal to take a polygraph examination would not prejudice one or become a part of his records.[51] Even though no federal legislation was adopted, the use of the polygraph by government agencies has been greatly curtailed as a result of the Moss Committee hearings.[52]

C. *Government Agencies' Love Affair with Electronic Gadgetry: The Long Subcommittee*

In 1965 and 1966 Senator Edward Long chaired the Subcommittee on Administrative Practice and Procedure of the Senate Committee on the Judiciary which held extensive hearings on invasions of privacy by government agencies.[53] Senator Long's committee submitted a lengthy questionnaire to thirty-four federal "non-security" agencies, asking the number and value of each kind of eavesdropping devices they had purchased during the last five years and what they were used for.[54] The committee found a great deal of

---

confessed and described how he must have done it. The bank was audited and the money allegedly taken was not missing. The manager was referred to a psychiatrist. In the course of examination it was revealed that the manager had guilt feelings about wrecking his mother's car and not reimbursing her for the damages of $800 to $1100. On the polygraph test, he had reacted to the question, "Have you ever stolen any money from the bank *or its customers*?" His mother was one of the bank's customers. *Hearings, supra* note 47, at 135-36.

50. Gallagher, *Privacy in the United States*, in B.C. ROWE, ED., PRIVACY, COMPUTERS, AND YOU (National Computing Centre, Ltd., Cheshire, England 1972).

51. H.R. REP. No. 89-198, *supra* note 48 at 2.

52. *See* A. WESTIN, PRIVACY AND FREEDOM at 396 (Athenum, N.Y. 1967). *See also*, SUBCOMM. ON CONSTITUTIONAL RIGHTS, SENATE COMM. ON THE JUDICIARY, 93RD CONG., 2D SESS., PRIVACY, POLYGRAPHS, AND EMPLOYMENT (Comm. Print 1974); *Hearings on the Use of Polygraphs and Similar Devices by Federal Agencies Before the Comm. on Foreign Operations and Government Information, House Comm. on Government Operations*, 93d Cong., 2d Sess. (1974).

53. *Hearings on Invasions of Privacy Before the Subcomm. on Administrative Practice and Procedure, Senate Comm. on the Judiciary*, 89th Cong. (1965-66). *See also* hearings held by the same committee on *Computer Privacy*, and the *Right of Privacy Act of 1967*, 90th Cong., 1st Sess. (1967).

54. *Hearings, supra* note 53, part 1 at 8-12. This list of agencies did not include the

hesitation, evasiveness, and uncooperation on the part of the agencies.[55] There was apparently good reason for such hesitation. The committees found that a large number of federal agencies used wiretapping despite federal laws, state laws, and agency regulations to the contrary.[56] These non-security agencies had invested in large quantities of expensive and sophisticated eavesdropping gear.[57]

The hearings of the Long Subcommittee also revealed widespread use of mail covers. A mail cover consists of recording the information found on the outside of an envelope. While postal officials insisted that no First Class Mail was being or could be opened without a search warrant, the subcommittee found the contrary.[58] Under the dubious legal authority of a "mail levy", mail was turned over to the Internal Revenue Service, which then opened the mail and seized the contents. As a result of the hearings, a law was passed forbidding the I.R.S. from opening First Class Mail, and new, more rigid regulations relating to mail covers were issued by the Postmaster General.

The Food and Drug Administration was particularly evasive and uncooperative. Outside witnesses, however, testified about FDA harrassment by inspections, bugging, raids and other methods of investigatory practices. In one incident, the FDA sent seven inspectors, a female undercover operator, and an array of electronic snooping equipment to a surburban supermarket to investigate two persons selling "Allerjoy", which allegedly did not contain sufficient protein content for a milk substitute.[59]

The Subcommittee found Internal Revenue Agents frequently violated federal and state laws and their own Department's clear and unequivocal policy directives banning wire taps. I.R.S. Special Agents admitted to illegal breaking and entering in order to install "bugs" for eavesdropping. The bugging of I.R.S. conference rooms with surreptitious recorders and two-way mirrors, in an attempt to intercept confidential conversations between taxpayers and their attorneys, was also revealed.[60]

Perhaps the most significant revelation to the Long Subcommittee was the fact that the Treasury Department sponsored a school, called a "technical aid school", at which IRS agents are

---

Department of Justice, the Department of Defense and the Central Intelligence Agency, the agencies directly responsible for law enforcement and security.

55. *Hearings, supra* note 53, part 1 at 3, part 4 at 1646, 1647.

56. *Hearings, supra* note 53, part 4 at 1644. *See also*, S. REP. No. 89-1053, 89th Cong., 2d Sess. (1966) at 4; S. REP. No. 90-1172, 90th Cong., 2d Sess. (1968) at 3.

57. *Id.*

58. *Id.* at 1645.

59. *Id.* at 1646.

60. *Id.*

trained in such arts as wiretapping, lockpicking and burglary.[61] Although the school was closed shortly after Senator Long revealed its existence, the IRS initially refused to allow the agents who attended the school to testify about its operation.[62] The IRS also admitted purchasing Bell Telephone Company trucks to be used for installing wiretaps.[63] Such surreptitious activity was unnecessary as the telephone company did not hesitate to accommodate the IRS, the FBI and local law enforcement agencies.[64]

Senator Long described a businessman threatened by industrial espionage who spends thousands of dollars having his office searched for electronic bugs every day, taking his phone apart each morning and stationing a special guard outside his office 24 hours a day.[65] The thought that all Americans would have to take similar precautions to protect their privacy from the Federal government is indeed a grisly one. But, as Senator Long stated,

> Unfortunately, electronic gadgetry has "grabbed" the law-enforcement community and given it what has been described as the Dick Tracy syndrome . . . . [M]any lawmen have fallen hopelessly in love with electronics and this romance is another problem standing in the way of curbing Big Brother.[66]

D. The Private Lives of Federal Employees: The Ervin Subcommittee

In 1966, Senator Sam Ervin, chairman of the Subcommittee on Constitutional Rights of the Senate Judiciary Committee, commenced hearings on privacy and the rights of federal employees.[67] Prospective federal employees, the subcommittee learned, had been subjected to probing interviews which covered highly personal matters. The subcommittee's report relates the experience of an 18 year old female who applied for a summer job as a secretary at the State Department, and was subjected to highly personal inquiries concerning intimate relationships. The girl's parents were so distraught when they learned of the interview that they had her withdraw her employment application, causing considerable financial hardship.

---

61. *Id.* at 1647.

62. *Id.* Some agents did later testify. *Id.* at 1999 *et seq.*

63. *Hearings, supra* note 53, part 3 at 1137.

64. *See* testimony of Arthur Brewster, division security supervisor, Southwestern Bell Telephone Co., *Id.* at 1845 *et seq.*

65. Long, *Right to Privacy*, 19 AD. LAW REV. 442, 444 (1967).

66. Long, *You Ought to be Left Along*, ESQUIRE, May, 1966.

67. *Hearings on Psychological Tests and Constitutional Rights Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 89th Cong., 1st Sess. (1965); *Hearings on Privacy and the Rights of Federal Employees*, before the same subcommittee, 89th Cong., 2d Sess. (1966). *See also*, other hearings held by the same subcommittee on *Privacy, the Census, and Federal Questionnaires*, 91st Cong., 1st Sess. (1969).

Both the girl and her mother were denied an opportunity to review what the interviewer had recorded in her file.[68]

The subcommittee also reported:

> In another case, the subcommittee was told, a woman was questioned for six hours "about every aspect of her sex life—real, imagined and gossiped—with an intensity that could only have been the product of inordinately salacious minds."[69]

Interference with employees' private lives continued after they were hired. For example, the president of the United Federation of Postal Clerks testified that low-paid postal clerks were "practically being ordered" to invest in U.S. Savings Bonds. A witness from another agency indicated that, in his agency, the names of individuals who did not participate in the savings bond drive were posted for all to see.[70]

The subcommittee was told of supervisors being ordered to supply the names of employees who attend P.T.A. meetings and engage in great books discussions. Evidence of outright intimidation, arm-twisting, and more subtle forms of coercion to obtain employee participation in particular programs was received by the committee. In addition to bond sale campaigns, Senator Ervin cited drives for charitable contributions, the use of self-identification minority status questionnaires, the sanctioning of polygraphs, personality tests, and improper questioning of applicants for employment.[71]

The subcommittee heard about "forced financial disclosure" where an employee must reveal details of his or his family's personal finances, debts, or ownership of property. Extensive questionnaires, sometimes taking six hours or more to answer, were required when no possible conflict of interest could be perceived.[72]

Senator Ervin was particularly critical of the new financial disclosure requirements. In reporting to the Senate he cited the case of an attorney threatened with disciplinary action or loss of his job because he was unable and unwilling to list all gifts—including Christmas presents from his family—which he had received in the past year. Senator Ervin pointed to the lack of procedures for appealing the decisions by supervisors and personnel officers which required such disclosure.[73]

At the conclusion of the hearings, Senator Ervin commented:

68. S. REP. No. 91-873, 91st Cong., 2d Sess. (1970) at 21. *See also*, S. REP. No. 90-534, 90th Cong., 1st Sess. (1967); S. REP. No. 92-554, 92d Cong., 1st Sess. (1971); and S. REP. No. 93-724, 93d Cong., 2d Sess. (1974).

69. *Id.* at 22.

70. *Id.* at 25.

71. *Id.* at 9.

72. *Id.* at 26.

73. *Id.* at 8.

> In view of some of the current practices reported by employee organizations and unions, it seems those who endorse these techniques for mind probing and thought control of employees have sworn hostility against the idea that every man has a right to be free of every form of tyranny over his mind: they forget that to be free, a man must have the right to think foolish thoughts as well as wise ones. They forget that the First Amendment implies the right to remain silent as well as the right to speak freely—the right to do nothing as well as the right to help implement lofty ideals.[74]

Bills to protect federal employees introduced as a result of this study are still being considered.[75]

E. Data Banks and Computers: The Gallagher, Long and Ervin Subcommittees

Hearings have been held by at least three separate committees on the threat to privacy posed by data banks and computers: the Special Subcommittee on Invasion of Privacy of the House Government Operations Committee chaired by Cornelius Gallagher in 1966;[76] the Subcommittee on Administrative Practice and Procedure of the Senate Judiciary Committee chaired by Senator Long in 1967;[77] and the Subcommittee on Constitutional Rights of the Senate Judiciary Committee chaired by Senator Ervin in 1971.[78]

The Gallagher Subcommittee reported that the Bureau of the Budget commissioned a feasibility study for the centralization and computerization of the many personal records now residing in individual agencies of the federal government. The resulting report, known as the Ruggles Report, recommended the immediate establishment of a Federal Data Center.[79] Two subsequent reports, the

---

74. *Id.*

75. S. 3703 and S. 3779 of the 89th Cong.; S. 1035 of the 90th Cong.; S. 782 of the 91st Cong.; S. 1438 of the 92d Cong.; S. 1688 of the 93d Cong.; H.R. 720, H.R. 1173, H.R. 1674, H.R. 4561, and S. 1887 of the 94th Congress. S. 1035, S. 782, S. 1438 and S. 1688 have been passed by the Senate. To date these bills have not cleared the House Post Office and Civil Service Committee, although extensive hearings have been held by the subcommittees of that committee. *Hearings on Privacy and the Rights of Federal Employees Before the Subcomm. in Manpower and Civil Service*, 90th Cong., 2d Sess. (1968); *Hearings on Invasions of Federal Employees' Privacy Before the Subcomm. on Retirement and Employee Benefits*, 92d Cong., 1st Sess. (1971); *Hearings on H.R. 1674* before the same subcommittee, 94th Cong., 1st Sess. (1975). A number of House bills on the same subject have also been introduced. *See e.g.* H.R. 17760 of the 90th Congress; H.R. 7969, H.R. 7199, H.R. 228, H.R. 294 of the 92d Congress; H.R. 12560 of the 93d Congress.

76. *Hearings on the Computer and Invasion of Privacy*, 89th Cong., 2d Sess. (1966).

77. *Hearings on Computer Privacy*, 90th Cong., 1st Sess. (1967). *See also*, by the same committee, GOVERNMENT DOSSIER, A SURVEY OF INFORMATION CONTAINED IN GOVERNMENT FILES, 90TH CONG., 1ST SESS. (Comm. Print 1967).

78. *Hearings on Federal Data Banks, Computers, and the Bill of Rights*, 92d Cong., 1st Sess. (1971).

79. H.R. REP. No. 90-1842, 90th Cong., 2d Sess. (1968).

Dunn report[80] and the Kaysen report,[81] endorsed the idea.

The proposal caused national alarm. As Congressman Gallagher explained, it could lead to "The Computerized Man" stripped of individuality and privacy as well as personal identity. "His life, his talent, and his earning capacity would be reduced to a tape with very few alternatives available."[82]

The Long Subcommittee embarked on a different course. That subcommittee sent a questionnaire to every federal department and agency requesting them to list the various types of information that could be consolidated into such a data bank. In the subcommittee's report, Senator Long explained:

> Let me briefly run down some of the immediate highlights of the Subcommittee survey. First, the Government keeps files on just about every imaginable bit of information on an individual's life—from the cradle to the grave. And the number of files is enormous. For example, Government reported that our names alone appeared in the files 2,800 million times. Our Social Security Numbers are listed 1,500 million times. Other figures include: Police records—264,500,000; Medical History—342 million; Psychiatric History—279 million.[83]

The proposed Federal Data Center was not adopted. But the threat to privacy caused by computers continues.

Senator Ervin's subcommittee held its hearings four years later. Like the Long Subcommittee, the Ervin Subcommittee sent out questionnaires to all federal departments and agencies, seeking to discover what kinds of automated information systems on citizens are being developed, for what purpose, and with what controls.[84] As in the case of the preceding questionnaire, Senator Ervin discovered great reluctancy on the part of federal agencies to release such information. The information he did receive was in some instances evasive and misleading.[85] Some of the information, however, was extremely revealing:

> Army surveillance of civilians engaging in political activities in the 1960's was both massive and unrestrained. At the height of the monitoring, the Army engaged over 1500 plainclothes agents to collect information which was placed in scores of data centers around the country. While most of the information collecting consisted of activities such as the clipping of newspaper accounts and

80. Edgar S. Dunn, Jr. of Resources for the Future, Inc.

81. Dr. Carl Kaysen, chairman, Institute for Advanced Study, Princeton University.

82. *Hearings, supra* note 76 at 2.

83. *Hearings, supra* note 77 at 2. A compilation of the survey results appears in the committee print GOVERNMENT DOSSIER, *supra* note 77.

84. *Hearings, supra* note 78 at 4.

85. *Id.*

> attending public events, there were many more serious instances of surveillance in which covert means were used to observe or infiltrate groups. No individual, organization, or activity which expressed "dissident views" was immune from such surveillance and, once identified, no information was too irrelevant to place on the Army computer.[86]

The results of this surveillance were widely distributed:

> To assure prompt communication of its agents' reports, the Command set up a nationwide teletype network devoted exclusively to internal security information. Completed at great expense in the fall of 1967, this secret wire service has, until recently, given the Pentagon, and each major troop command and intelligence unit in the United States, weekly, daily, and sometimes hourly reports on virtually all political protests wherever they have occurred. Courtesy copies of the reports were passed on to the FBI and to the Justice Department.[87]

A six volume mug book entitled *Individuals Active in Civil Disturbances* and known as the "Fort Holabird Blacklist" had been prepared for publication. It contained the names, pictures, and pertinent data of over one thousand persons, three to a page.[88] The computerized Biographical Data File contained dossiers on at least 4,078 persons. Various code numbers were devised to describe occupation, ideology and organizational affiliation. Among the 770 groups apparently politically suspect by the Army were many well known and highly respected organizations.[89] Although directives were issued by the Secretary of the Army and the Secretary of Defense to discontinue such surveillance and to destroy all of the existing files, the committee was uncertain whether this had been accomplished.[90]

---

86. SUBCOMM. ON CONSTITUTIONAL RIGHTS, SENATE COMM. ON THE JUDICIARY, 93D CONG., 1ST SESS., MILITARY SURVEILLANCE OF CIVILIAN POLITICS (Comm. Print 1973).

87. *Hearings, supra* note 78 at 187.

88. Comm. Print, *supra* note 86 at 50.

89. *Id.* at 62-65. The organizations included: American Civil Liberties Union, American Friends Service Committee, Americans for Constitutional Action, Americans for Democratic Action, Anti Defamation League of B'nai Brith, Christian Anti-Communist Crusade, Clergy and Laymen Concerned about Vietnam, Friends Committee on National Legislation, Fund for Republic, Inc., International Longshoremen's and Warehousemen's Union, International Union of Mine, Mill, and Smelter Workers, John Birch Society, League of Women Voters of the U.S.A., Liberal Party of New York, Mississippi Freedom Democratic Party, Moral Rearmament, National Association for the Advancement of Colored People, National Baptist Convention, U.S.A., Inc., National Committee for a Sane Nuclear Policy (SANE), National Council of Churches, National States Rights Party, National Urban League, Peace Corps, Ramparts, Religious Society of Friends, Southern Christian Leadership Conference, Student Non-violent Coordinating Committee, State Human Rights Commissions, Urban League, Women International Strike for Peace, Young Americans for Freedom, and Young Democrats.

90. *Id,* at 6, 62. *See also,* the follow-up hearings, *Hearings on Military Surveillance, Before the Subcomm. on Constitutional Rights, Senate Comm. on the Judiciary,* 93d Cong.

At least twenty-nine of the reported data banks were established to collect derogatory information about people.[91] Once information is collected, it is likely that it is readily passed on to other federal, state and local agencies; 92% of the data banks analyzed in the survey admitted sharing information with other agencies. Some maintained a regular list of "user agencies" authorized to gain full access to the data either by routine distribution or by computer interface.[92]

F. Arrest Records and Criminal Justice Data Banks: The Edwards and Ervin Subcommittees

A number of bills dealing with arrest records have been introduced in Congress.[93] Hearings on the subject were scheduled by a Subcommittee of the House Judiciary Committee (The Edwards Subcommittee) in 1972, 1973, and 1974.[94] Aryeh Neier, representing the American Civil Liberties Union, testified at these hearings about instances where persons had been damaged because of the dissemination of records of arrest without any indication of the subsequent disposition of the case.[95] According to the President's Commission on Law Enforcement and the Administration of Justice, 50% of the male citizens in this country will be arrested in their lifetime. For urban black males this figure may be as high as 90%.[96] Yet fewer than 25% are found guilty of the crime for which they were arrested, and fewer than 50% are found guilty of any offense.[97] Mr. Neier testified:

> Despite their innocence before the law, persons with an arrest record are subjected to the severe, continuing and pervasive punishment that attaches to the commission of a crime, namely the lifelong disabilities of a "criminal record." Furthermore, that disabil-

---

2d Sess. (1974). "Most of the intelligence reports on civilians prepared prior to 1971 apparently have been destroyed." Opening remarks of Senator Ervin, *Hearings* at 3.

91. SUBCOMM. ON CONSTITUTIONAL RIGHTS, SENATE COMM. ON CONSTITUTIONAL RIGHTS, SENATE COMM. ON THE JUDICIARY, 93D CONG., 2D SESS., SUMMARY AND CONCLUSIONS ON FEDERAL DATA BANKS AND CONSTITUTIONAL RIGHTS (1974) at 33.

92. *Id.* at 38. *See generally*, S. REP. No. 91-1205, 91st Cong., 2d Sess. (1970).

93. S. 2546, H.R. 10789, H.R. 10892, H.R. 13315 in the 92d Congress; S. 1906, S. 2542, S. 2810, S. 2963, S. 2965, S. 4252, H.R. 188, H.R. 9532, H.R. 7773, H.R. 12575, H.R. 9783, H.R. 12574, in the 93d Congress.

94. *Hearings on H.R. 13315 Before the Subcomm. No. 4 of the House Comm. on the Judiciary*, 92d Cong., 2d Sess. (1972). *Hearings on Dissemination of Criminal Justice Information Before the Subcomm. on Civil Rights and Constitutional Rights of the House Comm. on the Judiciary*, 93d Cong., 1st and 2d Sess. (1973-74).

95. *Hearings on H.R. 13315, supra* note 94 at 153; *Hearings on Dissemination, supra* note 94 at 78.

96. *Hearings on Dissemination, supra* note 94 at 96.

97. *Id.*

ity has the same damaging effect on a person's opportunity for employment and acceptance by society as a conviction record.[98]

For example, 75% of the employment agencies in the New York area will not accept for referral applicants with arrest records; sixty-six out of seventy-five employers surveyed would not consider hiring a man who had been arrested for assault even though he had been acquitted.[99]

In the Senate, Senator Ervin introduced S. 2963 "The Criminal Justice Information Control and Protection of Privacy Act of 1974", on the same day as Senator Hruska introduced the Administration's version for the same purpose, S. 2964. Hearings were held on these two bills, plus two other bills, starting in March, 1974, before Senator Ervin's Subcommittee on Constitutional Rights.[100]

Senator Ervin's statement presented to the Senate at the time he introduced S. 2963 outlined much of the concern. "Some of the most advanced technology is being used in local, state, and federal criminal justice data banks," he said.[101] The F.B.I. computer (National Crime Information Center), for example, can locate, reproduce and transmit to a remote terminal in California or Florida one of its 450,000 criminal histories in less than five seconds.[102] The project of making files on 21 million individuals instantaneously available to 40,000 state and local police departments will make the NCIC computerized criminal history one of the largest data bank information networks of personnel dossiers ever attempted.[103] It is not yet fully operational.

Senator Ervin cited the use of arrest information without the subsequent disposition of the case as one of the principal areas of abuse. He referred to several instances where local police and other officials have blindly followed instructions from "some faceless computer" to the serious detriment of an individual.[104]

---

98. *Id.*

99. *Id.* at 103.

100. *Hearings on Criminal Justice Data Banks—1974, Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 93d Cong., 2d Sess. (1974).

101. *Id.* at 15, 19.

102. *Id.* at 17.

103. *Id.* at 18.

104. One of the case histories involved a traffic violation. In Senator Ervin's words: Several months ago a young man was arrested by a local police department on a traffic charge. At first, he was told he could pay a $15 fine and would be released. But then an officer told him he could not leave because the Marines "had a hold on him." A detective then showed him a copy of a computer printout listing someone with the same name as AWOL from the Marines and a deserter. This young man was not AWOL or a deserter from the Marines because he was not even a Marine. The arrest occurred more than a month after the young man had become a civilian and his discharge papers attested to this. The assistant police chief said that the police were not to blame for the arrests—this had not been his first ar-

The sheer numbers of the files and names of individuals kept for law enforcement purposes by agencies of the federal government are staggering.

> For example, the Defense Department has several extensive files of very sensitive information, including dossiers on 1.6 million persons in its industrial security files. In the Justice Department alone, there is at least one civil disturbance file with 22,000 names; a file of approximately 250,000 names in the organized crime section; rap sheets or fingerprint cards on over 20 million individuals in the FBI's identification division files, and records on well over 450,000 persons in the FBI's National Crime Information Center—NCIC; and over 40 million names in the master index of the Immigration and Naturalization Service. The National Driver Register of the National Highway Safety Bureau contains 3,300,000 names. There are 69,000 names in the Secret Service files of persons considered potentially dangerous to the President, and the Secret Service computer contains hundreds of thousands of others.[105]

At the same time there appears to be no effective control on all of these files. For example, the "rap sheet" distribution system by the Identification Division of the FBI operates without formal rules. Rap sheets are made available to government licensing agencies, government personnel departments, and even to private employers. "Each day the Identification Division receives over 11,000 requests for record searches, a large portion of which are from non-law-enforcement agencies."[106] The problem is further compounded by a complete lack of control over the local law enforcement agencies receiving such information.

> For example, a few months ago a grand jury in Massachusetts began hearing evidence that State police officers were selling police records to department stores and other private businesses and credit agencies. This unfortunate abuse continues in case after case.[107]

A report by the Comptroller General on the use of criminal history information prepared at the request of Senator Ervin confirms the unauthorized use of such information in two of the three states analyzed.[108]

As Governor Francis Sargent explained to the committee, Massachusetts became a leader in protecting the privacy and security

---

rest—because they were only following the computer's instructions. (*Id.* at 15.)

105. *Id.* at 17.

106. *Id.* at 19.

107. *Id.*

108. *Id.* at 977.

of criminal records. In 1972, as a part of its attempt to computerize and update its criminal record system, it passed the first state law governing the privacy and security of criminal justice information systems.[109] As stated by the Governor, the four principles embodied in the statute are (1) regulation by statute and not by executive order, (2) restriction of access to law enforcement agencies, (3) limitation of data files to criminal convictions—no criminal intelligence or investigation information, and (4) the absolute right of an individual to see and correct his own file.

Even these simple standards caused difficulty for the State of Massachusetts. Federal agencies, including the FBI sought information in Massachusett's files but did not want to limit access to law enforcement agencies. When the state refused to join the FBI computer until similar restrictions were placed on the FBI's system, Massachusetts "felt the lash of Federal displeasure."

> The Small Business Administration threatened to withhold $30 million in disaster aid and loans. The Defense Department froze 2,400 jobs. The Justice Department brought suit against us.[110]

Although Massachusetts exerted some influence on the Federal system, it finally capitulated and joined the FBI's NCIC network in 1974.

G. Other Hearings

1. *Telephone Monitoring*

Even before the Moss Subcommittee commenced its inquiry into lie detector tests, it conducted a survey on telephone monitoring by government agencies. In its first report released in 1961, the subcommittee concluded that nearly every government agency permits secretaries to listen in on calls, or permits tape recording of such calls.[111]

Follow up surveys were made and nearly ten years later the same subcommittee reported that fifty-two out of sixty agencies surveyed permit telephone monitoring, an increase of eleven agencies. The practice is justified as an aid to greater efficiency. Pursuant to the subcommittee's request, most of the agencies have published regulations governing the practice and "usually" the per-

109. *Id.* at 51. Alaska, Arkansas, California, Iowa and Washington have now adopted similar statutes. These statutes are based on a model state law proposed by Project SEARCH, Technical Memorandum No. 3, May, 1971 (Cal. Crime Technological Research Foundation, 7171 Bowling Drive, Suite 190, Sacramento, Cal. 95823). *See* note 188 *infra*.

110. *Id.* at 52.

111. H.R. REP. No. 87-1215, 87th Cong., 1st Sess. (1961). *See also*, H.R. REP. No. 87-1898, 87th Cong., 2d Sess. (1962).

son making the call is told of the monitoring.[112]

Following press reports, the subcommittee also inquired into telephone service monitoring by telephone companies. The subcommittee was assured that the service monitoring did not include customer to customer conversations but only conversations necessary to determine whether a proper hookup was made.[113]

2. *Personality Tests*

In 1965 and 1966 a Special House Subcommittee on Invasion of Privacy, chaired by Congressman Cornelius Gallagher, held hearings inquiring into the use by government agencies of psychological or personality inventory tests. The subcommittee discovered a large number of agencies were using these tests on their employees and job applicants ostensibly to determine their emotional stability. Questions in such tests as the Minnesota Multiphasic Personality Inventory test asked about the individual's sex life, family situations, religious views, personal habits, childhood happenings, and other similar matters.[114] As a result of the hearings, many agencies either dropped the use of such tests altogether or greatly limited their use.[115]

3. *Mailing Lists*

The Subcommittee on Postal Operations of the House Post Office and Civil Service Committee commenced hearings on mailing lists in 1967.[116] Of the estimated 21 billion pieces of third class mail delivered each year, they discovered that over 15 billion were sent to addresses whose names were obtained from commercially

---

112. FOREIGN OPERATIONS AND GOVERNMENT INFORMATION SUBCOMM. OF THE HOUSE COMM. ON GOVERNMENT OPERATIONS, 91ST CONG., 2D SESS., AVAILABILITY OF INFORMATION FROM FEDERAL DEPARTMENTS AND AGENCIES (TELEPHONE MONITORING—THIRD REVIEW) (Comm. Print 1970). *See also, Hearings on Telephone Monitoring Practices by Federal Agencies Before the Foreign Operations and Government Information Subcomm. of the House Comm. on Government Operations*, 93d Cong., 2d Sess. (1974); *Hearings on FCC Monitoring of Employees' Telephones Before the Special Subcomm. on Investigations of the House Interstate and Foreign Commerce Comm.*, 92d Cong., 2d Sess. (1972).

113. Comm. Print, *supra* note 112 at 49.

114. *Hearings on a Special Inquiry on Invasion of Privacy, Before the Special Subcomm. on Invasions of Privacy of the House Comm. on Government Operations*, 89th Cong., 1st and 2d Sess. (1965-66).

115. For example, see the committment received by the committee from officers of the Peace Corps which had previously been using the entire MMPI for each of their applicants for overseas service. *Hearings, supra* note 114 at 237.

116. *Hearings on Registration of Mailing List Brokers with the Postmaster General*, 90th Cong., 1st Sess. (1967); *Hearings on Privacy in the Mail*, 90th Cong., 2d Sess., (1968); *Hearings on Mailing Lists (H.R. 2730 and Similar Bills)*, 91st Cong., 2d Sess. (1970); *Hearings on Obscenity in the Mail*, 91st Cong., 2d Sess. (1970).

available mailing lists.[117] Congressman Robert Nix, chairman of the Subcommittee, suggested that the mailbox is an extension of a person's home, and that force feeding it with that much third class mail is an invasion of privacy.[118]

Even more alarming, however, was the discovery that a large number of government agencies have joined the 250 commercial companies in the business of selling names. For example, Congressman Frank Horton, after a complaint from a constituent, discovered that the Internal Revenue Service would sell the list of 143,000 gun collectors obtained in the course of its administration of the gun registration laws to anyone who will pay the price, $140 or one tenth of a cent per name. Similarly, he found the Federal Communications Commission was selling the names and addresses of 265,000 amateur ham radio operators, the Federal Aviation Administration sells the lists of 680,000 licensed pilots, and the Coast Guard was selling the names of registered boat owners. In his survey of fifty agencies, he found many more also sold names on a regular basis.[119] Hearings were held on this subject in 1972.[120] Legislation prohibiting the sale or rental of mailing lists by federal agencies was finally adopted as a part of the Privacy Act of 1974.[121]

4. *Census Questions*

As early as 1940, the Bureau of the Census began receiving criticism for the questions it was asking on the decennial census. By 1970 the complaints were substantial. One of the questions raising much of the criticism was: "Do you have a bathtub or shower and . . . is it also used by another household."[122] A number of bills strengthening the confidentiality provisions and repealing the penalties for failing to answer were introduced but none passed.

The questions proposed for the 1970 Census of Population and Housing evoked considerable criticism. As a result, hearings were held by the Subcommittee on Census and Statistics of the House Post Office and Civil Service Committee.[123] It recommended that information on religious affiliation, social security number, the

117. See statement of Congressman Gallagher summarizing Exhibit I of the Postmaster General's cost ascertainment report for 1967 reproduced in *Hearings on Privacy in the Mail, supra* note 116 at 30.

118. *Id.* at 1.

119. *Hearings on the Sale or Distribution of Mailing Lists by Federal Agencies, Before the Foreign Operations and Government Information Subcomm. of the House Comm. on Government Operations*, 92d Cong., 2d Sess. (1972), at 28.

120. *Id.*

121. 5 U.S.C. § 552a(n).

122. H.R. REP. No. 93-246, 93d Cong., 1st Sess, (1973).

123. *Hearings on 1970 Census Questions*, 89th Cong., 2d Sess. (1966).

physically and mentally handicapped, and statistics on registration and voting be deleted.[124] However, neither H.R. 10952 nor the forty-four similar bills introduced in the 90th Congress to limit the categories of questions required to be answered under penalty of law in the Decennial Census of Population, Unemployment and Housing were passed. Similarly, none of the seventy bills introduced in the 91st Congress to do the same thing were successful.[125]

A number of hearings have been held on the subject.[126] The subcommittee has frequently stated that there has never been a claim substantiated that a census employee had ever divulged confidential information.[127] Bills introduced in the 92nd and 93rd Congress were similarly unsuccessful.[128]

5. *Consumer Credit Bureaus*

Congressman Gallagher's Special Subcommittee on Invasion of Privacy also considered the threat to privacy from consumer credit bureaus.[129] One of the witnesses, Professor Alan Westin, reported that over 2200 credit bureaus in the nation serve 400,000 "credit grantors" in 36,000 different communities. The Associated Credit Bureaus of America maintained credit files on more than 100 million individuals and issued 97.1 million reports in 1967.[130]

A number of bills were introduced for the purpose of enabling a person to protect himself against inaccurate and misleading credit information.[131] Additional hearings were held in 1968 and 1970 on the subject.[132] The result was the enactment of the Fair Credit Re-

---

124. H.R. REP. No. 93-246, *supra* note 122 at 9.

125. *Id.*

126. *Hearings on Privacy, the Census, and Federal Questionnaires Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 91st Cong., 1st Sess. (1969). Hearings before the Subcomm. on Census and Statistics of the House Post Office and Civil Service Committee, including: *Hearings, supra* note 123; *Hearings on 1970 Census Plans*, 90th Cong., 1st Sess. (1967); *Hearings on Limit Categories of Questions in Decennial Censuses*, 90th Cong., 1st Sess. (1967); *Hearings on the 1970 Census and Legislation Related Thereto*, 91st Cong., 1st Sess. (1969). *See also*, before the same subcommittee, *Hearings on the Mid-Decade Census*, 92d Cong., 1st Sess. (1971) and 93d Cong., 1st Sess. (1973); H.R. REP. No. 91-407, 91st Cong., 1st Sess. (1969).

127. H.R. REP. No. 93-246, *supra* note 122, at 3, 10; H.R. REP. No. 92-1288, 92d Cong., 2d Sess. (1972), at 2, 10.

128. The principal bills relating to confidentiality of the census were: H.R. 10952, of the 90th Congress; H.R. 20 of the 91st Congress; H.R. 14153 of the 92d Congress; and H.R. 7762 of the 93d Congress. *See* H.R. REP. No. 93-246, *supra* note 122.

129. *Hearings on Commercial Credit Bureaus Before the Special Subcomm. on Invasion of Privacy of the House Comm. on Government Operations*, 90th Cong., 2d Sess. (1968); *Hearings on Retail Credit Co. of Atlanta, Georgia*, 90th Cong., 2d Sess. (1968), before the same subcommittee.

130. *Hearings on Commercial Credit Bureaus, supra* note 129 at 5.

131. *See e.g.* H.R. 6071, H.R. 16340, and S. 823 of the 91st Congress.

132. *Hearings on the Credit Industry Before the Subcomm. on Antitrust and Monoply*

porting Act which was attached as a Senate Amendment to the Bank Secrecy Act of 1970.[133] The Fair Credit Reporting Act, attached to the Consumer Protection Act of 1968 (Truth in Lending Act) limited the use of credit reports, required deletion of obsolete information, required disclosure of the information in the file to the consumer upon request, and required the disclosure of the source of the credit report to the consumer if it was used to deny credit.[134] Additional hearings have been held on the same subject since the enactment of the Fair Credit Reporting Act.[135]

6. *The FBI's "COINTELPRO"*

Activities of the F.B.I.'s counterintelligence program began to come to light after an F.B.I. office in Media, Pennsylvania, was broken into in 1971 and a large number of F.B.I. documents began appearing in the press shortly thereafter. A law suit under the Freedom of Information Act was brought by NBC newsman Carl Stern, and Chairman Peter Rodino of the House Judiciary Committee started requesting further information from the F.B.I. and the Justice Department. Finally, the "Peterson Report" prepared by Henry Peterson was presented to the Subcommittee on Civil Rights and Constitutional Rights (Edwards Subcommittee) of the House Judiciary Committee outlining the various activities of the so-called "COINTELPRO" operations.[136]

The report outlines the following FBI activities directed to various "leftist" and extremist groups undertaken on the justification of counter-intelligence: (1) Sending anonymous or fictitious materials to cause disruption; (2) Dissemination of public record information to media sources to expose the groups; (3) Leaking investigative information to the news media; (4) Advising local authorities of civil and criminal violations; (5) Using informants to disrupt a group's activities by sowing dissention and exploiting disputes; (6) Informing employers, credit bureaus and creditors of members' activities for the purpose of adversely affecting their employment and credit; (7) Informing businesses and business associates of members for the

---

of the Senate Comm. on the Judiciary, 90th Cong., 2d Sess. (1968); *Hearings on H.R. 16340 and S. 823 Before the Subcomm. on Consumer Affairs of the House Comm. on Banking and Currency*, 91st Cong., 2d Sess. (1970).

133. Act of October 26, 1970; P.L. 91-508, Title VI; 84 Stat. 1128; 15 U.S.C. § 1681.

134. 16 U.S.C. § 681 *et seq.*

135. *Hearings on the Fair Credit Reporting Act of 1973 Before the Subcomm. on Consumer Credit of the Senate Comm. on Banking, Housing, and Urban Affairs*, 93d Cong., 1st Sess. (1973); *Hearings on Credit Reporting Abuses*, 93d Cong., 2d Sess. (1974), before the same subcommittee.

136. *Hearings on FBI Counter-Intelligence Programs Before the Subcomm. on Civil Rights and Constitutional Rights of the House Comm. on the Judiciary*, 93d Cong., 2d Sess. (1974) at 1.

same purpose; (8) Interviewing and contacting members to recruit paid informants; (9) Persuading religious and civic leaders to help disrupt the group activities; (10) Disrupting the political or judicial process involving members of the target groups; (11) Establishing sham organizations for disruptive purposes; (12) Informing the family or other persons of the radical or immoral activity of group members; (13) and miscellaneous other activities (such as investigating the love life of a group leader for dissemination to the press).[137] According to Attorney General William Saxbe, the counter-intelligence activities were stopped in 1971.[138]

On August 1, 1975, it was announced that a secret list, known as the "security index," was maintained by the FBI. This list contained the names of 15,000 Americans targeted for detention in the event of a national emergency. It was compiled to be used under the Subversive Activities Control Act. Even though the applicable provisions of that Act were repealed in 1971, the security index was still being maintained in anticipation of reinstatement of such authority.[139]

7. *The Watergate and Ellsberg Break-ins*

The break-in by the "Plumbers" (the name given to the special White House intelligence group) at the Democratic National Headquarters in the Watergate Complex touched off the Watergate scandal. The break-in at the office of Daniel Ellsberg's psychiatrist, apparently in an attempt by the White House to obtain some sensational evidence to use against the person who released the Pentagon Papers, was only one more of a large number of other shocking disclosures. The Congressional hearings on wiretapping, surveillance, break-ins, examination of income tax returns and other invasions of privacy by officers or agents of the White House are voluminous.[140] Senator Ervin sums up the message of Watergate as follows:

> Yet if we have learned anything in this last year of Watergate, it is that there must be limits upon what the Government can know about each of its citizens. Each time we give up a bit of information

137. *Id.* at 13-15.

138. *Id.* at 9.

139. "F.B.I. Reportedly Listed Citizens to Detain in Crisis," *N.Y. Times*, Aug. 3, 1975, p. 1.

140. *Hearings on Watergate and Related Activities Before the Senate Select Comm. on Presidential Campaign Activities* (Ervin Committee), 93d Cong., 1st Sess. (1973); *The Impeachment Inquiry of the House Comm. on the Judiciary*, 93d Cong., 2d Sess. (1974); *Hearings Relating to an Inquiry into the Alleged Involvement of the CIA in Watergate and Ellsberg Matters Before the Special Subcomm. on Intelligence of the House Armed Services Comm.*, 93d Cong., 1st and 2d Sess. (1973-74).

about ourselves to the Government, we give up some of our freedom. For the more the Government or any institution knows about us, the more power it has over us. When the Government knows all of our secrets, we stand naked before official power. Stripped of our privacy, we lose our rights and privileges. The Bill of Rights then becomes just so many words.[141]

8. *The Collinsville Incident*

Watergate was not the only revelation of privacy invasion by officers and agents of the federal government. On April 23, 1973, a number of officers of the Bureau of Narcotics and Dangerous Drugs, dressed in the clothes of the drug culture and brandishing sawed-off guns and pistols, forced their way into the homes of two families in Collinsville, Illinois, without advance warning or search warrants. They terrorized the families by holding them at gun point, using foul and threatening language, and preventing them from calling the police while ransacking their homes. Upon discovery of their mistake, the officers left without so much as a word of sorrow or apology. A full description of the incident and the resulting medical problems it caused (twenty weeks' hospitalization in one case) was given in testimony before a House subcommittee in May of 1973.[142]

9. *Inspection of Farmers' Income Tax Returns*

By an executive order dated January 17, 1973[143] President Nixon authorized the Department of Agriculture to inspect more than 3 million Federal income tax returns of farmers and extract certain personal financial information of the taxpayer for the purposes of compiling special mailing lists to make statistical surveys. When it was discovered, and recognized as the first time an entire class of citizens were singled out for such disclosure, several congressional inquiries were made into the practice authorized by the executive order.[144] During the hearings the Justice Department admitted that the order was intended to be a model for use by other agencies also seeking personal financial information from individual income

141. *Hearings, supra* note 100 at 16.

142. *Hearings on Reorganization Plan No. 2 of 1973 Before the Subcomm. on Reorganization, Research, and International Organizations of the House Comm. on Government Operations*, 93d Cong., 1st Sess. (1973).

143. Exec. Order No. 11697, later modified by Exec. Order No. 11709 dated March 27, 1973.

144. *Hearings on Inspection of Farmers' Federal Income Tax Returns by the U.S. Department of Agriculture Before the Subcomm. on Department Operations of the House Agriculture Comm.*, 92d Cong., 1st Sess. (1973); *Hearings on Executive Orders 11697 and 11709 Before the Subcomm. on Foreign Operations and Government Information of the House Comm. on Government Operations*, 93d Cong., 1st Sess. (1973).

tax returns.[145] On March 22, 1974, at the recommendation of then Vice President Ford, the authorization was withdrawn and the original executive order revoked.[146]

10. *Other Privacy Invasions*

The House and Senate have conducted hearings and sponsored studies into a wide variety of subjects in the area of invasion of privacy including: the so-called Bank Secrecy Act;[147] Treasury Department admissions that once a complaint of violence focused on a particular suspect, the Department sometimes checked library cards to see if the suspect read books on explosives and revolutionary activity;[148] federal information systems, and how technology affects them;[149] the controversial "no-knock" provision authorizing entry of a home by law enforcement officers without first knocking and announcing their authority;[150] the use of behavior modification drugs in grammar school children;[151] the use and distribution of medical records;[152] the use of information in drug abuse data banks;[153] and political intelligence in the Internal Revenue Service.[154]

H. The Buckley Amendment and the Privacy Act of 1974

1. *The Buckley Amendment*

The first major breakthrough in the field of legislation to pro-

145. *Id.* at 9.

146. Exec. Order No. 11773, 3A C.F.R. 133.

147. 12 U.S.C. §§ 1829b, 1730, 1951-59, and 31 U.S.C. §§ 1051-1122. *See Hearings on Amendments to the Bank Secrecy Act Before the Subcomm. on Financial Institutions of the Senate Comm. on Banking, Housing, and Urban Affairs*, 92d Cong., 2d Sess. (1972); *Hearings on the Effect of the Bank Secrecy Act on State Laws*, 93d Cong., 2d Sess. (1974), before the same subcommittee.

148. *Hearings on Riots, Civil, and Criminal Disorders Before the Senate Comm. on Government Operations*, 91st Cong., 2d Sess. (1970), at 5358.

149. *Hearings on Government Information Systems and Plans Before the Foreign Operations and Government Information Subcomm. of the House Comm. on Government Operations*, 93d Cong., 1st and 2d Sess. (1973-74).

150. H.R. REP. No. 91-1444, 91st Cong., 2d Sess. (1970), at 86. The law was passed in 1970, 21 U.S.C. §§ 801-879. However, the controversial no-knock provision was later dropped, 21 U.S.C. § 879.

151. *Hearings on Federal Involvement in the Use of Behavior Modification Drugs on Grammar School Children Before the Special Studies Subcomm. of the House Comm. on Government Operations*, 91st Cong., 2d Sess. (1970).

152. H.R. REP. No. 92-1007, 92d Cong., 2d Sess. (1972).

153. SUBCOMM. ON CONSTITUTIONAL RIGHTS OF THE SENATE COMM. ON THE JUDICIARY, 93D CONG., 2D SESS., DRUG ABUSE DATA BANKS, (Comm. Print 1974).

154. SUBCOMM. ON CONSTITUTIONAL RIGHTS OF THE SENATE COMM. ON THE JUDICIARY, 93D CONG., 2D SESS., POLITICAL INTELLIGENCE IN THE INTERNAL REVENUE SERVICE, (Comm. Print 1974). *See also, Hearings on the Constitutional Immunity of Congressional Members Before the Joint Comm. on Congressional Operations*, 93d Cong., 1st Sess. (1973).

tect personally identifiable information in government files was the adoption of the "Buckley Amendment". Senator James L. Buckley of New York attached his "Family Education Rights and Privacy Act of 1974" to the omnibus education bill which was signed into law on August 20, 1974.[155]

As amended, the Buckley Amendment requires all educational institutions or agencies receiving federal funding of any kind to allow parents to inspect and review the education records of their children. Parents must have an opportunity to correct or delete any inaccurate or inappropriate information. Except for identifying data, called directory information, personally identifiable information cannot be made available to persons not specifically authorized to receive it without consent of the parents. Other school officials and officials of an institution to which the student makes an application for admission or financial aid are specifically authorized to receive the information. A record of each access must be kept by the institution and must be available to the parents.

Further, under the Buckley Amendment, a student accedes to all the rights of his parents once he becomes eighteen or enrolls in an institution of post-secondary education. The parents or student must be informed of their rights under the Act. The penalty for violation is loss of federal funds. The Act provides for a review board to insure compliance and adjudicate violations.[156] Additionally, the Secretary of Health, Education and Welfare is required to adopt regulations protecting privacy of persons in connection with any surveys or data gathering activities of the Department and any educational institution.[157] Under the December 31, 1974 amendments, financial records of the parents, confidential letters of recommendation written prior to January 1, 1975, employment records, law enforcement records separately kept, and medical records are excepted from the operation of the act.[158]

2. *The Privacy Act of 1974*

A number of bills on privacy were introduced in the 92nd and 93rd Congress. Most of these were aimed at the dossiers and records maintained by government agencies. In June of 1972 and February, April and May of 1974, hearings were held on the subject in the House.[159] The result was a committee bill, HR 16373, introduced by

155. P.L. 93-380, Title V, § 513(a), 88 Stat. 571. *See* 20 U.S.C. § 1232g. The Act was further amended by P.L. 93-568, § 2(a), 88 Stat. 1858 (1974).

156. 20 U.S.C. § 1232g.

157. 20 U.S.C. § 1232g(c).

158. P.L. 93-568, § 2(a); 20 U.S.C. § 1232g.

159. *Hearings on Records Maintained by Government Agencies Before the Subcomm.*

the subcommittee chairman, Congressman William Moorhead.[160]

In the Senate, hearings were held jointly by the Ad Hoc Subcommittee on Privacy and Information Systems and the Subcommittee on Constitutional Rights in June of 1974.[161] Senator Sam Ervin chaired both subcommitees; the bill under discussion was S. 3418 sponsored by Senator Ervin. The committee report heralds the bill as an "Information Bill of Rights" for citizens and a "Code of Fair Information Practices" for departments and agencies.[162] The Senate version prevailed and it was signed by the President on December 31, 1974, as the Privacy Act of 1974.[163]

The principle substantive provisions of the act (§ 3) appear as an amendment to the Administrative Procedure Act, immediately following the section of the A.P.A. containing the Freedom of Information Act. The Privacy Act covers the collection, storage and use of personal information, but applies to federal agencies only.

Under the act, no agency may disclose a personally identifiable record without the written consent of the individual to whom the record pertains, unless the use is routine and to officers and employees of the agency. There are exceptions for disclosure to the Bureau of the Census, the National Archives, any agency for civil or criminal law enforcement, Congress, the Comptroller General, and any person for health and safety purposes (provided a subsequent notice is sent to the individual to which the record pertains).[164] The date, nature, and purpose of each disclosure plus the name and address of the recipient must be recorded and kept for five years.[165]

Any individual has a right to review his own record and obtain a copy upon payment of the reproduction costs. He may request an amendment to his record which must be granted or denied within 10 days. The denial can be appealed to the agency head and then to a federal district court. Any disclosure after the request is submit-

---

on Foreign Operations and Government Information of the House Comm. on Government Operations, 92d Cong., 2d Sess. (1972); *Hearings on Access to Records*, 93d Cong., 2d Sess. (1974), before the same subcommittee. *See also, Hearings, supra* note 149.

160. *See* H.R. REP. No. 93-1416, 93d Cong., 2d Sess. (1974).

161. *Joint Hearings on Privacy: Collection, Use and Computerization of Personal Data Before the Senate Ad Hoc Subcomm. on Privacy and Information Systems of the Senate Comm. on Government Operations and the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 93d Cong., 2d Sess. (1974). *See also*, jointly by the same sub-committees, PRIVACY AND PROTECTION OF PERSONAL INFORMATION IN EUROPE, 93d Cong., 2d Sess. (Comm. Print 1975).

162. S. REP. No. 93-1183, 93d Cong., 2d Sess. (1974), at 5. *See also*, SENATE COMM. ON GOVERNMENT OPERATIONS, 93D CONG., 2D SESS., MATERIALS PERTAINING TO S. 3418, (Comm. Print 1974).

163. Act of Dec. 31, 1974; P.L. 93-579; 88 Stat. 1896; 5 U.S.C. § 552a.

164. *Id.* at § 552a(b).

165. *Id.* at § 552a(c).

ted must note the dispute.[166] This access requirement does not apply to the Central Intelligence Agency, the National Archives, law enforcement agencies, nor does it apply to records kept for internal use only, for law enforcement purposes, for providing protective services to the President, or for statistical purposes. Finally, it does not apply to certain investigatory or evaluation material to the extent the material was received upon a promise to keep the source confidential. It does not apply to testing material used for appointment or promotion in Federal Service if the disclosure would compromise the objectivity of the testing process. In each case, however, the exemption is not effective unless the agency in question has a specific rule providing such an exemption along with the reasons for the exemption.[167]

The act requires each agency to limit its records to information which is relevant and necessary, to collect information directly from the subject individual if possible, and to give each individual supplying information a written statement of the purpose and authority for collecting the information, the uses to which it will be put, and the effects of not providing the information. A description of the system along with a description of the routine uses of the records, the policies and practices of the agency, the name of the individual responsible, the procedures for individual access and the sources must be published in the Federal Register at least annually. Before using or disseminating any record the agency must determine the accuracy, relevance, timeliness and completeness of any information about an individual. There is an absolute ban on maintaining a record describing how any individual exercises his First Amendment rights unless authorized by statute or done in connection with authorized law enforcement activity. Rules of conduct and security safeguards must be devised to insure security and confidentiality of the records.[168]

Federal District Courts have authority to order compliance with any of the act's provisions upon an action brought by an individual. It can award costs and reasonable attorney's fees to the individual if he prevails and actual damages, in no case less than $1000, if the violation is willful or intentional. Willful violations are punishable as a misdemeanor with a fine not to exceed $1000.[169]

The act prohibits the sale or rental of mailing lists by any federal agency.[170] Notice to Congress and the Office of Management

166. *Id.* at § 552a(d).
167. *Id.* at § 552a(j), (k) and (l).
168. *Id.* at § 552a(e).
169. *Id.* at § 552a(g) and (i).
170. *Id.* at § 552a(n).

and Budget must be given before establishing or altering any information record system to permit adequate evaluation of the proposal.[171] The President must submit a report to Congress each year listing the exemptions declared by each agency and reasons for each exemption.[172]

Section 7 of the Privacy Act of 1974 prohibits any federal, state, or local government agency from denying anyone any right or benefit because of his refusal to disclose his social security number. The only exceptions are disclosures required by federal statute and disclosures required by state law or regulation prior to January 1, 1975.[173]

Finally, a seven member commission known as the "Privacy Protection Study Commission" is established. It is charged with making a study of all data banks, governmental and private, and with recommending how the principles of the Privacy Act of 1974 should be applied to those systems which are not already covered. It is further specifically directed to study mailing lists, transfers of information by the Internal Revenue Service, and whether the federal government should be liable for damages for violation of the act. The report is to be prepared in two years at which time the commission is to be dissolved.[174]

3. *A Postscript on Congressional Action*

Congressional attention to privacy is far from concluded with the passage of the Buckley Amendment and the Privacy Act of 1974. In the first seven months of the 94th Congress, at least seventy-three bills have been introduced dealing with the subject. The Subcommittee on Courts, Civil Liberties and Administration of Justice of the House Judiciary Committee held hearings on the "Mosher-Mathias Bill" (H.R. 214) which would require a court order based on probable cause for any surveillance—by telephone, bank records, mail, etc.—by federal agents. It was opposed, among others, by FBI Director Clarence Kelley. A House Government Operations subcommittee has received an internal report on the Internal Revenue Service undercover activity including "illegal activities." The Subcommittee on Bank Supervision of the House Banking and Currency Committee commenced hearings on bills to protect bank customer confidentiality (amendments to the Bank Secrecy Act) (H.R. 1005 and H.R. 7483) on July 16, 1975. Senator Proxmire, chairman

171. *Id.* at § 552a(o).
172. *Id.* at § 552a(p).
173. P.L. 93-579 § 7, ___ U.S.C. ___, 5 U.S.C.S. § 552a note.
174. *Id.*

of the Senate Banking Committee, has introduced his amendments to the Fair Credit Reporting Act of 1970 (S. 1840). And a one-day hearing was held by the Subcommittee on Constitutional Rights of the Senate Judiciary on June 23, 1975, into reports of a possible link-up among the personal files of the FBI, Treasury Department, Defense Department, and other federal agencies.[175]

Ironically, although some progress has been made in Congress, Congress has taken some steps backward at the same time. As it was passing the Privacy Act of 1974 limiting the use of the social security number, it was also amending the Social Security Act to require all welfare recipients to disclose social security numbers as a condition of receiving benefits. In the same law, H.E.W. is required to establish a computerized Parent Locator Service with authority to tap the Internal Revenue Service records and records from any other agency to find the last known address of an absent parent not supporting his child. States will be required to set up comparable locators.[176]

It appears that Congress' admonition on the expanded use of social security numbers is having little impact on the Supreme Court across the street. The names and social security numbers of all attorneys authorized to practice before the Court are being computerized along with the case load, statistics, and correspondence.[177]

IV. Privacy in the Executive Branch

A. *Criminal Justice Information Systems and Project Search*

1. *Project SEARCH and Computerized Criminal Histories*

In a report entitled "The Challenge of Crime in a Free Society," the President's Commission on Law Enforcement and Administration of Justice recommended, in 1967, the immediate establishment of a nationwide computer-based information systems network to keep track of criminal offenders and for more effective use of existing criminal justice resources.[178] The next year the Law Enforcement Assistance Administration (LEAA) was created as a part of the Omnibus Crime Control and Safe Streets Act of 1968.[179] This new agency immediately concluded that there was a "central need" for the development of a uniform format for criminal history records—one that could be used by all elements of the criminal justice

175. Privacy Journal, *supra* note 41 at 2.
176. 42 U.S.C. § 651 *et seq.*
177. Privacy Journal, *supra* note 41 at 2.
178. U.S. Gov't Printing Ofc., Feb. 1967, at 266.
179. 42 U.S.C. § 3701 *et seq.*

system including police, courts, and corrections.[180] Thus, in 1969 LEAA funded Project SEARCH (System for Electronic Analysis and Retrieval of Criminal Histories), a project coordinated by the California Crime Technological Research Foundation and directed primarily by ten participating states—later expanded to twenty states. Eventually participation was extended to representatives of all fifty states, Puerto Rico, the Virgin Islands, and the District of Columbia. Project SEARCH quickly developed and tested a prototype system for the exchange of criminal histories on a national basis. In doing so, however, Project SEARCH heeded the strong advice of the President's Commission on Law Enforcement and Administration of Justice to retain the centralized national computer as an index only, allowing the principle exchange of information to take place between local agencies. Further, both the President's Commission and Project SEARCH recommended definite safeguards to protect the privacy of individual records.[181]

Project SEARCH recommended this national index system be separate from the FBI's National Crime Information Center (NCIC) which had instantaneous retrieval capability for stolen property and wanted persons information. Attorney General John Mitchell, however, decided to centralize the system in 1970 and placed it under operational control of the FBI despite objections from LEAA and Project SEARCH.[182] Thus, the Computerized Criminal History (CCH) became the eighth item added to the NCIC computer. When the NCIC Board approved the CCH system in March of 1971, the index concept was dropped. Instead, each criminal history was to contain a complete detailed record of the offender—basically the same information contained in the "rap sheet" previously maintained manually by the FBI. This step was justified as an interim measure because not all states would participate in the system at the beginning, which would make the "index" concept partially ineffective.[183]

Once a central system was designed, Project SEARCH turned

180. Richard W. Velde, Associate Administrator, the Law Enforcement Assistance Administration, remarks, in *Proceedings of the International Symposium on Criminal Justice Information and Statistics Systems* (Sponsored by Project SEARCH and The Law Enforcement Assistance Administration), Oct. 3-5, 1972, New Orleans, Louisiana at 16.

181. *The Challenge of Crime in a Free Society, supra* note 178 at 268; Project SEARCH, *Security and Privacy Considerations in Criminal History Information Systems*, Technical Report No. 2, July, 1970 (Cal. Crime Technological Research Foundation, 7171 Bowling Drive, Suite 190, Sacramento, Cal. 95823).

182. Drabe Lundell, Jr., *Computerized Criminal Histories: A 7-Year Blunder?* COMPUTERWORLD, July 17, 1974, at 11.

183. The other items in the NCIC computer are (1) wanted persons, (2) stolen vehicles, (3) stolen license plates, (4) stolen articles, (5) stolen guns, (6) stolen securities, and (7) stolen boats. *See Hearings, supra* note 100 at 9.

its attention to the implementation of supportive systems at the local level. Upon completion of the design for a statewide criminal justice statistics system and demonstration of a prototype, Project SEARCH proceeded to implement its model in five of the original participating states.[184] From the very beginning, however, Project SEARCH was concerned about security and privacy. During the initial organization of the project a Security of Records Subcommittee was formed. Later a Security and Privacy Committee was created which drafted a Code of Ethics and made various other recommendations for limiting access, use and dissemination of the collected data. These recommendations were officially approved by the committee and published in its second report in July 1970.[185]

The next step of the Security and Privacy Committee of Project SEARCH was to draft a model state act for criminal offender record information for adoption by its participating states and other states. This task was completed in May of 1971.[186] Under this model act a Criminal Offender Records Control Committee is established which is charged with creating a continuing program of data auditing and verification to assure accuracy and completeness, adopting regulations to assure security of the information from unauthorized disclosure, and adopting regulations to preserve anonymity in connection with any use of the information for research purposes. Access would be limited to criminal justice agencies and others authorized by state statute. An individual would be guaranteed the right to inspect and challenge any information contained in the system that relates to him. Civil liabilities and criminal penalties would be established for violations including automatic damages of $100 to $1000 plus attorney's fees for willful violations. Additionally, a Security and Privacy Council would be established to conduct an ongoing investigation of ways and methods to improve the security and privacy of the system.[187] Although every state has been requested to establish a task force or special committee to study this model act and recommend legislation to their respective legislatures, to date Massachusetts, Alaska, Arkansas, California and Iowa

184. The five states are: California, Florida, Michigan, Minnesota, and New Jersey. *See* Project SEARCH: *Designing a Statewide Criminal Justice Statistics Systems—The Demonstration of a Prototype*, Technical Report No. 3, November, 1970; *Implementing Statewide Criminal Justice Statistics Systems—The Model and Implementation Environment*, Technical Report No. 4, January, 1972; *Designing a Statewide Criminal Justice Statistics Systems—An Examination of the Five State Implementation*, Technical Report No. 5, December, 1972.

185. Technical Report No. 2, *supra* note 181.

186. Technical Memorandum No. 3, *supra* note 109.

187. *Id.*

are the only states to adopt legislation patterned on this model act.[188]

A few months later, this same committee prepared and published model administrative regulations for adoption in the states. These regulations elaborate on many of the principles established in the model act. Additionally, they provide for closing the record after five years with no activity and expunging the record if required by other law or regulation or upon request of the state which originally supplied the information. Each criminal justice agency is required to maintain a list of all persons to which it releases information. The information contained in a record system would be classified according to its sensitivity and a personnel clearance system would be established giving greater protection for that information deemed highly sensitive. The computers should be dedicated to criminal justice use only, if at all possible.[189]

The Security and Privacy Committee also have prepared a model "Terminal Users Agreement" for use by a centralized state agency and each of the local criminal justice agencies authorized to receive computerized criminal information.[190] Finally, the Committee has prepared a memorandum on criminal justice computer hardware and software security considerations designed to assist administrators in dealing with computer venders.[191]

2. *Federal Regulations*

The work of the Security and Privacy Committee of Project SEARCH came to the attention of Senator Edward Kennedy and in July of 1973 he and Senator John McClellan introduced an amendment to the Crime Control Act of 1973 requiring LEAA to issue regulations to control the dissemination of criminal history information by state criminal justice agencies which received LEAA funds. The amendment specifically refers to inclusion of disposition of arrests, keeping the information current, and review and challenge by individuals affected.[192]

---

188. MASS. GEN. LAWS, ch. 6, §§167 to 178; AK. STAT. §§ 12.62.010 to 12.62.070 (1962); ARK. STAT. ANN. §§ 5-832 to 5-841 (Supp. 1973); CAL. PEN. CODE §§ 11075 to 11144, § 1203.45, § 2947 (West 1972); IOWA CODE ANN. §§ 749B.1 to 749B.20 (Supp. 1974). *See Project, Government Information and the Rights of Citizens*, 73 MICH. L. REV. 971 (May-June, 1975).

189. Project SEARCH, *Model Administrative Regulations for Criminal Offender Record Information*, Technical Memorandum No. 4, March, 1972.

190. Project SEARCH, *Terminal Users Agreement for CCH and Other Criminal Justice Information*, Technical Memorandum No. 5, November, 1973.

191. Project SEARCH, *Criminal Justice Computer Hardware and Software Considerations*, Technical Memorandum No. 6, January, 1974. *See also, Proceedings, supra* note 180.

192. 42 U.S.C. § 3771(b).

Regulations pursuant to the Kennedy Amendment were to become effective June 19, 1975.[193] Under the regulations, each state agency collecting, storing, or disseminating criminal history record information with the help of LEAA funds must submit a plan to LEAA for approval within 180 days. Approval guidelines require updating arrest records within 90 days of the disposition of the arrest, require limitations on dissemination (particularly if no disposition appears one year after arrest or if the record pertains to a juvenile), require annual audits, require certain security measures, and require right of access and review by individuals. The most controversial portion of the regulations was the requirement that any computers used to handle criminal history record information be dedicated to such purposes. The Justice Department and LEAA yielded to the pressure of state governments alarmed at the cost of dedicated computer systems and agreed to drop this requirement in proposed regulations published on October 24, 1975.[194] Additionally, the regulations restated the FBI Security and Confidentiality doctrine which has governed participation in the NCIC computer.

Based largely on the concepts developed by the Security and Privacy Committee of Project SEARCH, the NCIC Advisory Policy Board established guidelines for participation by the states in the NCIC/CCH system. All state terminals have been obliged to contract by written agreement to abide by all rules, policies and procedures of the NCIC Advisory Policy Board. Under the heading "Security and Confidentiality" the Advisory Policy Board limits input to serious and significant violations excluding certain named offenses, limits input to official record entries of offenses, limits access largely to law enforcement agencies, requires law enforcement control over the computers, and guarantees the individual's right to review and challenge the contents of his record. Also the security and confidentiality doctrine requires continuous checks on records to insure accuracy, completeness, and the security of the records from unauthorized use.[195]

193. 39 Fed. Reg. 5636 (Feb. 14, 1974) and 40 Fed. Reg. 22114 (May 20, 1975). Under the regulations the approved plan was to be fully operational and implemented by December 31, 1977. However, that portion relating to the right of access and review by individuals was to be fully operational and implemented upon submission of the original plan within 180 days or by December 16, 1975. The Department of Justice and LEAA have now published new proposed regulations in the Federal Register which postpone the submission of the plan and the implementation of the right of access and review until March 16, 1976. 40 Fed. Reg. 49789 (Oct. 24, 1975) § 20.21.

194. *Id.*

195. National Crime Information Center (NCIC) Computerized Criminal History Program, Background, Concept, and Policy as Approved by NCIC Policy Board, September 13, 1973.

At least one state was unable to meet these policy guidelines. In July 1974 the NCIC Advisory Policy Board voted to remove the state of New York from the system. New York had refused, after numerous warnings, to update its information; it failed to follow up the arrest information with disposition of the case. The New York information, nearly 45,500 entries or approximately one tenth of all the entries in the computer at the time, was simply purged from the disks at NCIC. At the same time Pennsylvania voluntarily withdrew from the system claiming it was too expensive.[196]

The long standing FBI practice of sharing information on criminal records with federally chartered or insured banking institutions came to an abrupt halt when a federal court judge in the District of Columbia prohibited the FBI from distributing arrest records to banks contributing fingerprints to the FBI in *Menard v. Mitchell*.[197] Within months, however, the practice was reinstated by the passage of the "Bible" amendment to the Justice Department's appropriations bill.[198] The same amendment attached by the House Appropriations Committee to the 1972 FBI appropriations bill was stricken at the insistence of Senator Ervin.[199] Hence the current status of the legal authorization of the practice is not clear. The FBI did, however, announce that effective July 1, 1974, it will not include arrest data more than one year old not accompanied by dispositions in responding to any requests by banking institutions.[200]

3. *Preparation of Proposed Federal Legislation*

Congress adopted the Mathias Amendment to the Omnibus Crime Control and Safe Streets Act which became law on January 2, 1971. It provided that LEAA shall submit to the President and Congress by May 1, 1971, recommendations for legislation to promote integrity and accuracy of criminal justice data collection and to protect the constitutional rights of all persons affected by the system.[201] As a result of this mandate, the administration intro-

196. COMPUTERWORLD, July 3, 1974.

197. 328 F. Supp. 718 (D.C.D.C. 1971). *See* Sec. 19 of Federal Deposit Insurance Act, 12 U.S.C. § 1829, which prohibits persons convicted of crimes involving dishonesty or breach of trust from serving as directors, officers, or employees of insured banks.

198. Act of Dec. 15, 1971; P.L. 92-184, § 902. Senator Bible of New Mexico sponsored the amendment.

199. *See* Mark Gitenstein, "The Issue of Security and Privacy," in *Proceedings, supra* note 180. Senator Ervin and Senator Bible had reached a compromise agreement which was then inserted into the Senate version. However, the conference committee struck this compromise language from the bill altogether. The administration's bill, S. 3834, to allow dissemination of criminal records by the FBI with certain important limitations, was not acted upon in the 92d Congress.

200. 39 Fed. Reg. 23057, June 20, 1974.

201. 18 U.S.C. § 3767.

duced S. 2546 of the 92nd Congress, with Senator Roman Hruska as chief sponsor. This bill was generally criticized as failing to provide adequate protection against misuse of data or invasion of privacy and was not acted upon.[202] In the 93rd Congress, the Administration introduced a new bill also sponsored by Senator Hruska, S. 2964. Although extensive hearings were held on this bill along with a companion bill introduced by Senator Ervin, Congress again failed to act. The same bill was introduced in the 94th Congress as H.R. 61. It is still pending.

4. *National Advisory Commission on Criminal Justice Standards and Goals*

Another project funded by LEAA that relied heavily on the Project SEARCH security and privacy materials is the National Advisory Commission on Criminal Justice Standards and Goals. This commission and its four operational task forces and eight advisory task forces, representing a cross section of criminal justice leaders and experts from state and local government as well as from the private sector, produced six major reports containing approximately 2500 pages and approximately 500 detailed standards and recommendations.[203] The commission was conceived as a part of LEAA's charge under the Omnibus Crime Control and Safe Streets Act of 1968 to encourage research and development directed toward improvement of criminal justice and encouraging states to adopt comprehensive plans. The standards are strictly advisory and cannot be made a prerequisite for funding or any other assistance. Nevertheless, each state has been invited to review the standards by their own advisory commissions and take whatever steps may be necessary to encourage the implementation of these standards and goals. The specific recommendations are taken from, and largely correspond with, the security and privacy guidelines recommended by the Security and Privacy Committee of Project SEARCH.[204]

B. The H.E.W. Report: Automated Data Processing and The Social Security Number

A discussion of the significant H.E.W. study must start with a discussion of the Social Security number. The Social Security num-

202. *Hearings on Dissemination, supra* note 94 at 78.

203. Executive Summary—Reports of the National Advisory Commission on Criminal Justice Standards and Goals, Department of Justice, LEAA, U.S. Gov't Printing Off. 1974. The six reports are entitled (1) A National Strategy to Reduce Crime, (2) Police, (3) Courts, (4) Corrections, (5) Community Crime Prevention, and (6) Criminal Justice Systems.

204. NATIONAL ADVISORY COMMISSION ON CRIMINAL JUSTICE STANDARDS AND GOALS, CRIMINAL JUSTICE SYSTEM (Washington, D.C. 1973) at 114.

ber first came into existence when the implementation of the new Social Security Act commenced in 1936. Its utility as a means of helping to sort information accurately among the records of a large number of persons, many of whom have identical or similar names, became evident to many other people, both in and out of government. In 1943 the Civil Service Commission requested and obtained an executive order from President Roosevelt mandating the use of the Social Security number by all other Federal agencies as the means of organizing individual account records.[205] Gradually, most agencies of the federal and state government that have had large-scale individual record-keeping requirements have come to use the social security number. The same applies to similar agencies of local government and many private organizations.

The use of the Social Security number has become so widespread in this country that it is rapidly becoming a standard universal identifier.

> A cross-section of . . . complaints appearing in the [ad hoc Subcommittee on Privacy and Information Systems] hearings shows that people are pressured in the private sector to surrender their numbers in order to get telephones, to check out books in university libraries, to get checks cashed, to vote, to obtain drivers' licenses, to be considered for bank loans, and many other benefits, rights or privileges.[206]

During the hearings on "Federal Data Banks, Computers and the Bill of Rights," Senator Ervin quipped:

> They tell us when we leave this world we take nothing with us, but I expect I will take my Social Security card. I am just afraid if I got up to the Pearly Gates—if I get that far toward Paradise—St. Peter might not let me in unless I can show my number.[207]

Finally, the American National Standards Institute (ANSI) proposed that the individual's name and Social Security number be made the standard form of identification of individuals for purposes of data interchange.[208] The importance of such a standard in the computer age where a simple code enables complete interfacing of whole data banks is immediately apparent.[209]

---

205. Exec. Order No. 9397.

206. S. REP. No. 93-1183, 93d Cong., 2d Sess. (1974), at 29.

207. *Hearings, supra* note 78 at 787.

208. Martin, "The Issue of Security and Privacy", *Proceedings, supra* note 180.

209. For example, the single item that brought by far the most critical comments upon introduction of H.B. 1024 (43d Legislative Assembly, State of Montana) by this author, was a ban on the use of the Social Security number without statutory authorization. Nearly every state agency in the State of Montana suggested they could not function without the use of Social Security numbers.

The Social Security Administration did not immediately respond to ANSI's request to make the Social Security number the standard form of identification of individuals in this country. Instead a task force was appointed in March of 1970. This task force concluded that the policy issues involved were beyond the reach of the Social Security Administration and recommended that the Secretary of Health, Education and Welfare create a public advisory body to examine these issues further.[210] Even before this task force had completed their report, however, Secretary Elliot Richardson, in his testimony before Senator Ervin's Subcommittee investigating federal data banks and computers, proposed to appoint an advisory group to review the broader problems connected with the use of the Social Security number and to develop effective safeguards against the abuse of the number by others.[211] Before the advisory committee was appointed, the Secretary decided the Social Security number was "just a proxy for other sources of concern" and that the committee would have to address the whole range of issues connected with the application of automated data processing technology to the needs of our modern society.[212]

In April of 1971 Secretary Richardson established the Secretary's Advisory Committee on Automated Personal Data Systems. The Committee took testimony from over one hundred witnesses and studied the work that was being done on the same subject in Canada[213] and Sweden.[214] Its report was released in July, 1973.[215]

The report has been widely heralded. It has been the basis of much legislation introduced in Congress[216] and in state legislatures.[217] The new privacy law in Minnesota is patterned after the

---

210. Martin, *supra* note 208.

211. Hearings, *supra* note 78 at 787.

212. Martin, *supra* note 208 at 558.

213. TASK FORCE ON PRIVACY AND COMPUTERS OF THE CANADIAN DEPARTMENT OF COMMUNICATION AND CANADIAN DEPARTMENT OF JUSTICE, PRIVACY AND COMPUTERS (Ottawa, Information Canada, 1972).

214. SWEDISH COMMITTEE ON AUTOMATED PERSONAL SYSTEMS, DEPARTMENT OF JUSTICE, DATA AND PRIVACY, (Stockholm, Almanna Forlaget, 1972). *See* Appendix B of the Report, note 215 *infra* at 167 for actions taken by other countries.

215. REPORT, SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (U.S. Gov't. Printing Ofc. 1973).

216. *See e.g.*, H.R. 10042, H.R. 14493 and H.R. 15526 and S. 2810 of the 93d Congress; H.R. 1984, H.R. 3235, H.R. 3236, H.R. 3237, H.R. 7234 of the 94th Congress.

217. *See e.g.*, H.B. 1024 of the 43d Session and SB 389, SB 400 of the 44th Session in the Montana Legislature (introduced by this author); AB2656 of the 1973-74 Session in the California Legislature; Code of Fair Information Practices in the Ohio Legislature; H-6106 in the Washington Legislature; S. 233 of the 1975 Session in the Utah Legislature. *See also*, bills introduced in Massachusetts, Michigan, Delaware, Arkansas, Ohio, Indiana, Nebraska, Kansas, Rhode Island and Pennsylvania discussed in *Privacy Legislation: Analysis of Alternatives*, a report prepared by McCaffery, Seligman and von Simson, Inc., 251 East 61st Street, N.Y.C. 10021 (1975).

recommendations of the report.[218] The model act prepared by the National Association for State Information Systems (NASIS) and Government Management Information Sciences (G-MIS) follows many of its recommendations.[219] It was used as a base for drafting the Privacy Act of 1974 recently enacted by Congress.[220] In particular the Privacy Act prohibits any governmental agency from denying anyone any right or benefit because of his refusal to disclose his Social Security number.[221]

The report concludes that a person's privacy is poorly protected against arbitrary or abusive record-keeping practices under current law. It recommends the enactment of a federal "Code of Fair Information Practice" for all automated personal data systems resting on five principles: (1) There must be no personal data record-keeping systems the existence of which is secret. (2) There must be a way for an individual to find out what information about him is in a record and how it is used. (3) There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent. (4) There must be a way for an individual to correct or amend a record of identifiable information about him. And, (5), any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.[222]

The recommendations proposed by the report and intended to form the basis of such a code are divided into two sets of safeguard requirements; one for administrative automated personal data systems, and one for automated personal data systems used exclusively for statistical reporting and research. In general they restrict the transfer of personal data into an automated system without consent, require the identification of a person responsible for the system, require action to inform employees of the safeguards, prevent disciplinary action against anyone disclosing noncompliance, require precautions to protect the data from threats or hazards, restrict the transfer of data from one computer to another without consent, require a record of each access, require accuracy, completeness, timeliness and pertinence, require elimination of outdated data, re-

218. MINN. STAT. ANN. § 15.162 *et seq.* (1964).

219. *See* a description of the model act in *NASIS States: Model Bill to Promote Privacy of State Government Banks*, GOVERNMENT DATA SYSTEMS, May-June, 1974, at 6.

220. *See* S. REP. No. 93-1183, 93d Cong., 2d Sess. (1974) at 8; H.R. REP. No, 93-1416, 93d Cong., 2d Sess. (1974) at 7.

221. *Supra* note 173.

222. REPORT, *supra* note 215 at xx and xxi.

quire availability of sufficient information to allow an independent analysis of research data, require public notice of the existence and character of the system once each year, require informing the individual of the consequences for refusing to furnish requested data, require the data to be made available to the individual to which it pertains upon request, limit the use to the use originally contemplated without consent, require informing the individual of all uses made of the data upon request, require notification of the individual before release of data pursuant to a court order, and require procedures to allow the individual to challenge the accuracy of data about himself. These safeguard requirements should, the report recommends, be adopted by administrative regulation by agencies for application to all systems within reach of their authority pending the adopting of a Code of Fair Information Practices.

Additionally, the report recommends that a standard universal identifier should not be established in the United States. Until the safeguard requirements are fully effective, the Social Security number should not be used for any purpose other than those contemplated by federal law unless specifically authorized by Congress. Unless authorized by Congress, no one should be coerced into using the Social Security number or lose a benefit because he refuses to disclose it. There should be no positive program for issuing Social Security numbers to children below the ninth grade level. Finally the report recommended federal legislation specifically prohibiting use of the Social Security number for promotional or commercial purposes.[223]

C. The President's Privacy Address and the Domestic Council Committee on the Right to Privacy

In his State of the Union address on January 30, 1974, President Nixon listed protecting the right of personal privacy for every American as one of the ten key areas in which landmark accomplishments were possible in 1974.[224] In his message, the President suggested that the problem is limiting the uses to which private information is put and recognizing the basic proprietary rights each individual has in information concerning himself. He announced an "extensive Cabinet-level review" of both government and industry practices relating to privacy.[225] These comments were followed within the

223. *Id.* at xxiii (Summary of Recommendations) and 48.

224. Nixon, *State of the Union Address*, 10 PRESIDENTIAL DOCUMENTS 113, 115 (1974). The Democratic response by Senate Majority Leader Mike Mansfield also mentioned the importance of protecting privacy.

225. Nixon, *The State of the Union Message to Congress*, January 30, 1974, 10 PRESIDENTIAL DOCUMENTS 122, 136 (1974).

month by a radio address to the nation devoted solely to privacy.[226]

The President announced the creation of the Domestic Council Committee on the Right of Privacy. Described as "no ordinary group", the President appointed Vice President Ford as chairman of the committee, and six cabinet officers as members. The committee was directed to produce action to "provide a personal shield for every American which he can use to protect his right to privacy."[227]

Senator Philip Hart, delivering the official Democratic response to President Nixon's radio address, suggested that if the President wanted to "live up to the rhetoric of his message" he should: (1) order an end to all political spying and support current legislation to prohibit military personnel from spying on American citizens; (2) order a stop to all wiretapping, bugging or breaking and entering without an independent court order; (3) order an end to the use of "national security" to hide or excuse illegal acts; (4) order an end to the practice of federal agencies secretly obtaining telephone records, bank records and other private business records without a subpoena; and (5) support stiffer controls on dissemination and use of criminal justice records than contained in the Administration's criminal justice information bills.[228]

The American Civil Liberties Union responded with an eleven page "Program to Safeguard Individual Privacy" which was intended as a "blueprint" for both Congress and the Executive Branch. Among the more novel suggestions of the A.C.L.U. was the one requiring privacy impact statements before establishing new federal programs.[229]

The Domestic Council Committee on the Right of Privacy decided to take action and support implementation of work already done rather than undertake another study. At its first meeting on July 10, 1974 it approved fourteen "initiatives". The initiatives included: (1) The Office of Consumer Affairs in the White House should develop a "Declaration of Consumer Rights to Privacy" and urge private business to voluntarily subscribe to a code of fair information practices. (2) The Fair Credit Reporting Act should be strengthened to allow greater control over the information by individuals affected. (3) Privacy impact statements should be required for present and future federal data banks that contain personal

226. Nixon, *The American Right of Privacy, Address on Nationwide Radio*, February 23, 1974, 10 PRESIDENTIAL DOCUMENTS 245 (1974).

227. *Id.* at 246.

228. Senator Philip Hart, Radio Text of Congressional Response to President Nixon's Message on Privacy, March 2, 1974.

229. *Memorandum: A Program to Safeguard Individual Privacy*, American Civil Liberties Union, 410 First St. S.E., Washington, D.C. 20003 (Feb. 1974).

information. (4) All federal data banks should pass a compliance test to assume proper safeguarding of personal information. (5) The committee endorsed the concepts in H.R. 16373 which later became the basis of The Privacy Act of 1974. (6) Specific studies should be undertaken by federal agencies concerned with banking and retailing concerning the privacy implications of electronic funds transfer and point-of-sale systems. (7) The Office of Management and Budget should issue regulations requiring all agencies to establish procedures for informing people of their rights when asked to furnish personal information about themselves. The committee also: (8) endorsed the sections of the Buckley Amendment allowing inspection of school records by students and parents; (9) endorsed the idea of a federal employees' bill of rights to privacy; (10) supported the requirement of a subpoena or court order for inspection of bank records; (11) supported legislation that would prohibit military spying on civilian activities; (12) endorsed legislation that would prohibit cable television companies from giving out information on subscribers; (13) recommended that all forms seeking information for any federal agency contain a check off box to allow individuals to prohibit the sale of their names for mailing list purposes; and (14) endorsed the Internal Revenue Service plans to develop stronger, more comprehensive legislation to protect taxpayer records.[230]

Three days after President Gerald Ford took office, in his address to Congress and the nation, he pledged:

> There will be no illegal tappings, eavesdropping, bugging or break-ins by my Administration. There will be hot pursuit of tough laws to prevent illegal invasions of privacy in both government and private activities.[231]

In view of the past activities of the federal government, that may prove a difficult pledge to keep.

D. The Rockefeller Report on the C.I.A.

This article would not be complete without a discussion of the recently released Rockefeller Report on the Central Intelligence Agency. The public charges of wrongdoing and extralegal activities on the part of the C.I.A. became so strong that President Ford was obliged to create a special commission to investigate these activities on January 4, 1975.

The specific charges were that: (1) large-scale spying on Ameri-

230. Domestic Council Committee on the Right of Privacy, Fact Sheet on Meeting of Committee, July 10, 1974. *See also*, E.D. Lundell, *Ford Council Pushes Federal Regulation*, COMPUTERWORLD, July, 1974.

231. 10 PRESIDENTIAL DOCUMENTS 1029, 1034.

can citizens in the United States was conducted by the C.I.A. whose responsibility was foreign intelligence; (2) dossiers on large numbers of American citizens were kept; (3) many of these activities were aimed at Americans who had expressed their disagreement with government policies; (4) personal mail had been intercepted and opened in the United States over the last twenty years; (5) domestic dissident groups had been infiltrated; (6) the C.I.A. had engaged in illegal wiretaps, and break-ins; and (7) the C.I.A. had improperly assisted other government agencies.[232] Although the Commission attempted to soften the impact of its conclusions by stating that "the great majority of the C.I.A.'s domestic activities comply with its statutory authority," many of the charges were found to be true.[233]

For example, the Commission found that in August 1967 a Special Operations Group was formed to collect, coordinate, evaluate and report on foreign contacts with American dissidents. This group later became known as Operation CHAOS. Within six years CHAOS had compiled some 13,000 different files including files on 7,200 American citizens. The names of more than 300,000 persons and organizations were included in these and related materials, all of which were entered into a computerized index.[234]

The report showed that the C.I.A. was, in fact, intercepting and reading mail of U.S. citizens. By 1959 the mail opening project included the opening of over 13,000 letters a year. Photographic equipment was apparently installed in Post Offices; the letters were opened, photographed, resealed and sent on their way. Other organizations, such as the F.B.I., furnished names of persons to place on watch lists which contained in excess of 600 names including those of American citizens. In the last full year of its operation, 4,350,000 items of mail were handled by the New York intercept office.[235]

The report documents the assistance given to E. Howard Hunt and various members of the White House staff in the Watergate and Ellsberg affairs. The C.I.A. provided alias documents and disguise materials, a tape recorder, camera, film and film processing to E. Howard Hunt. It prepared a psychological profile of Daniel Ells-

232. COMMISSION ON CIA ACTIVITIES WITHIN THE UNITED STATES, REPORT TO THE PRESIDENT, (June, 1975) (Manor reprint N.Y.C.) at 9. *See also, CIA: Who's Watching Whom*, NEWSWEEK, June 23, 1975, at 19.

233. *Id.* at 10.

234. *Id.* at 130. The nearly 1000 "subject" files on numerous organizations included such organizations as Student Non-Violent Coordinating Committee (SNCC), Students for a Democratic Society (SDS), Women's Strike for Peace, American Indian Movement (AIM), Woman's Liberation Movement, National Mobilization Committee to End the War in Vietnam, the Black Panther Party, and Clergy and Laymen Concerned about Vietnam. *Id.* at 144.

235. *Id.* at 101.

berg; however, the commission found no evidence that the C.I.A. knew of the break-in to Dr. Fielding's office in advance.[236]

In an effort to insure its own security, the Office of Security of the C.I.A. has engaged in wiretapping, bugging, surreptitious entries and other improper conduct.[237] For example, physical surveillance of one C.I.A. employee was conducted for almost one year. A surreptitious entry was made into his apartment by cutting through the walls from an adjacent apartment for the purpose of installing microphones. A mail cover was placed on his mail and his income tax returns were reviewed. No evidence of disloyalty was found.[238] In two cases the telephones of three newsmen were tapped in an effort to identify the sources of sensitive intelligence information. Reporters were followed in an effort to identify their sources in three other instances. Occasionally, American citizens not connected with the C.I.A., and other government employees, were placed under surveillance or investigated.[239]

The C.I.A.'s activities remain under investigation in Congress. The House has appointed a Select Committee on Intelligence under the chairmanship of Congressman Otis Pike. The Senate has appointed a Special Committee to Study Governmental Operations with Respect to Intelligence Activities under the chairmanship of Senator Frank Church.

V. Privacy in Montana

A. *The Montana Supreme Court*

The Montana supreme court has decided two important privacy cases. The first, the 1952 case of *Welsh v. Roehm*,[240] firmly established the right of privacy as grounds for a tort action in Montana. In that case, the court affirmed the award of $250.00 exemplary damages to a tenant whose landlord moved into the tenant's living room and remained there with his wife for seventeen days and nights. The court had no difficulty in finding an invasion of the tenant's privacy by the landlord. Similarly, it had no serious difficulty in finding a right of privacy as "a part of the right to liberty and pursuit of happiness" and as "within the absolute rights of

236. *Id.* at 172.

237. It later developed that the CIA kept information on crimes committed by CIA agents secret. According to agency documents made public on July 22, 1975, information on at least nine cases involving crimes committed by CIA agents were withheld by the CIA under a secret agreement with the Justice Department. N.Y. Times, July 23, 1975, at 16, col. 1.

238. Report, *supra* note 232 at 164.

239. *Id.* at 164.

240. 125 Mont. 517, 241 P.2d 816 (1952).

personal security and personal liberty."[241]

In 1971, the Montana supreme court decided an equally significant case, *State v. Brecht*.[242] This case involved the conviction of the defendant for the murder of his wife. The conviction was based in part upon the admissibility of testimony of his wife's sister who surreptitiously overheard a threat to the deceased by the defendant on an extension phone. The Montana supreme court, quoting extensively from *Welsh v. Roehm*, found this secret eavesdropping on a telephone conversation between a husband and wife to be a violation of the defendant's Fourth Amendment rights under the federal Constitution. As such, it was within the scope of the exclusionary rule, even though the violation was committed by a private person, and not by law enforcement officers.

B. The 1972 Montana Constitution

The adoption of two sections relating to privacy in the 1972 Montana Constitution placed Montana in the forefront of states dealing with the question of privacy.[243] To date, there have been no significant Supreme Court decisions interpreting the privacy provisions of either of these two sections.[244] They have, however, been the subject of opinions by the Attorney General. For example, the Attorney General stated that the exception from the right to know which reads, "except in cases in which the demand of individual privacy clearly exceeds the merits of public disclosure," protects corporations as well as natural persons.[245] The Attorney General has also stated that the publication of a list of delinquent taxpayers in a newspaper for purposes of embarrassment was a violation of Article II, Section 10 of the 1972 Montana Constitution.[246]

Perhaps the most helpful guide for interpretation of Montana's new constitutional provision on privacy comes from the Committee Report of the Bill of Rights Committee in the Constitutional Convention. The report states in part:

> The Committee believes the Constitution should specify that the only circumstance in which the right of privacy may be infringed is following the showing of a compelling state interest. This is in response to the increasing concern expressed nationwide that the

241. *Id.* at 819.

242. 157 Mont. 264, 485 P.2d 47 (1971).

243. See *supra* notes 33 and 34 and accompanying text.

244. Privacy was obviously involved in *Gazette Printing Co. v. Carden*, 163 Mont. 401, 517 P.2d 361 (1973), but the court never reached that question.

245. 36 MONT. ATT. GEN. OP., Opinion No. 28, 35 MONT. ATT. GEN. OP.; Opinion No. 59.

246. 35 MONT. ATT. GEN. OP., Opinion No. 62.

> fear of individual privacy is in danger of eclipse in an advanced technological society. The point of this provision is not to prohibit all invasions of privacy, but to require that no invasion of privacy should occur until and unless a compelling state interest has been established.[247]

C. *Legislation*

The Constitutional Convention clearly contemplated legislation implementing the constitutional provision on the right of privacy:

> The committee proposed a broad provision in this area to permit flexibility to the courts in resolving the tensions between public interests and privacy. It is hoped that the Legislature will have occasion to provide additional protection for the right of privacy in explicit areas where safeguards are required.[248]

In 1973, the Legislature adopted a section in the new Criminal Code on "privacy in communications" which was largely a recodification of the old law on obscene phone calls, tampering with telegraph and telephone lines, and the unauthorized reading of sealed letters.[249] It does include a prohibition against disturbing, by repeated telephone calls, the right of a person's privacy and the recording of any conversation without consent of all parties to the conversation unless the recording is done by public officials, at public meetings, or with proper warning.

A statute prohibiting the use of lie detector tests as a condition for employment or continuation of employment was passed in the 1974 session of the Legislature.[250] However, this provision was limited to mechanical lie detector tests or polygraph tests and specifically did not apply to public law enforcement agencies.[251]

Additionally, the Legislature has begun to use a clause providing that "the demands of individual privacy outweigh the merits of public disclosure" in statutes dealing with the confidentiality of government records.[252]

Comprehensive legislation to implement Article II, Section 10 of the new Montana Constitution was introduced in 1974 as House Bill 1024 by this author, entitled, "The Montana Privacy Act."

---

247. Comments, Bill of Rights Committee Proposal, Montana Constitutional Convention, 1972, at 24.

248. *Id.*

249. REVISED CODES OF MONTANA (1947) [hereinafter cited as R.C.M. 1947] § 94-8-114.

250. R.C.M. 1947, § 41-119.

251. R.C.M. 1947, §§ 41-119 and 41-120.

252. *See e.g.*, R.C.M. 1947, § 84-7308, dealing with confidentiality of information required by the Realty Transfer Act.

House Bill 1024 was a comprehensive measure that divided the subject of privacy into the following four categories: (1) Privacy of the home and other private places; (2) Privacy of communications; (3) Privacy of the mind; and (4) Privacy of the marriage and family.

In the first part, entry by any person into the home of another was made unlawful unless the entry was made under one of several exceptions such as consent, entry under the authority of a valid search warrant, entry by a landlord at reasonable times, or entry in cases of an emergency.

Privacy of communications provisions would have outlawed interception of communications in progress (wiretapping, eavesdropping, interception of the mails, and mail covers) as well as barring disclosure of certain privileged communications after the communication has taken place (doctor-patient privilege, attorney-client privilege, priest-penitent privilege, counselor-counselee privilege, husband and wife privilege, and a privilege for communications among parents and children).

Privacy of the mind and personality provisions would have protected a person's thoughts, sentiments, emotions, sensations, religious beliefs, philosophical beliefs, and political beliefs from improper disclosure or publication. This part would have banned loyalty oaths (except oaths using the language of the Constitution), disclosure of organizational affiliation, lie detector tests and questioning under the effect of thiopental sodium or other chemical substance, psychological personality inventory tests, certain probing employment questions, and commercial exploitation of a person's name, picture, or portrait. The bill contained safeguards against dissemination of arrest records, unreasonable surveillance, surveillance at a political meeting, and keeping records of persons attending a political meeting. Additionally, this category of privacy would have included the safeguards for automated personal data systems developed by the HEW Report, including protection against abuse of the Social Security number.[253]

Finally, in the last category, marital or family privacy, the bill recognized the right of a married couple to decide for themselves whether to procreate children, use birth control devices, and to do any other acts or make any other choice consistent with the marital relationship. The parents' full control over the religious training and guidance of their children would be protected.

The bill specifically provided for criminal penalties for violation of the Act and a civil action by the victim for actual damages, not less than $200.00 per violation, and punitive or exemplary dam-

253. *See supra*, text accompanying note 205 *et seq.*

ages if applicable, along with reasonable attorney's fees.

The bill passed the House with little difficulty, but died in the Senate Judiciary Committee in the final days of the session. The bill was reintroduced as Senate Bill 400 in the 1975 session. The portion relating to automated personal data systems was separated and introduced as Senate Bill 389 of the 1975 session. Both bills were reported favorable by the Senate Judiciary Committee, but killed on the floor of the Senate although substantial amendments were made at the request of the law enforcement community and retail merchants. A proposal to study the issue was accepted by the Priorities Committee as a third priority for the Interim Joint Committee on the Judiciary. The Interim Committee hopes to hold its first session on privacy in the summer of 1976.

D. Criminal Justice Information Systems

In early 1974, the Montana Board of Crime Control established a task force on privacy and security. Upon establishment of the Council on Criminal Justice Standards and Goals, it became the Information Systems Task Force charged with the responsibility of reviewing and drafting standards and goals for Criminal Justice Information Systems in Montana.[254] In May of 1975, the task force split into two groups, one continuing as a part of the Council on Criminal Justice Standards and Goals and the other as a Criminal Justice Information System Advisory Committee to the Board of Crime Control. This latter committee was charged with the responsibility of drafting privacy and security legislation in the area of arrest records and criminal justice information systems and to otherwise assist in the implementation of the Federal Regulations promulgated by LEAA.[255]

On October 10, 1975, the Criminal Justice Information System Advisory Committee adopted model regulations for use by all Montana Criminal Justice Agencies to implement Section 20.21(g)(1-6) of the regulations promulgated on May 20, 1975, pursuant to the authority of the Crime Control Act of 1973.[256] These model regulations provide access by individuals to their criminal history record information and further provide procedures for review and correction of such information. They specifically provide for methods of verification, costs and fees, the type of information that must be made available, the procedure for correction, and the establishment of a three-member board outside the criminal justice agency for

254. *See supra*, text accompanying note 203 *et seq*.
255. *See supra*, text accompanying note 192 *et seq*.
256. *Supra* note 122.

purposes of appellate review. Although not all city and county legislative bodies have formally adopted the regulations as contemplated, most local law enforcement agencies in the state have indicated their willingness to comply with these access and review requirements.